Deutscher Bundestag
9. Wahlperiode

Drucksache 9/2386

13. 01. 83

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Fünfter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/7 — vom 13. Januar 1983 gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes.

Fünf Jahre Arbeit für den Datenschutz und der bevorstehende Ablauf einer Amtszeit sind Anlaß genug, eine Zwischenbilanz zu ziehen. Dieser fünfte Tätigkeitsbericht, den ich dem Deutschen Bundestag vorlege, behandelt deshalb nicht nur die Kontroll- und Beratungstätigkeit im Jahre 1982, sondern er versucht zugleich die Entwicklung von Datenverarbeitung und Datenschutz über die letzten Jahre hin darzustellen, soweit dies aus der Sicht des Bundesbeauftragten und im Rahmen seiner Zuständigkeit möglich ist. Ich möchte damit auch einem Wunsch des Bundestags-Innenausschusses entgegenkommen, der mich in der Beschlußempfehlung vom 10. März 1982 zu meinem Zweiten und Dritten Tätigkeitsbericht (Drucksache 9/1623) ersucht hat, in künftigen Berichten jeweils auf offengebliebene Fragen und Forderungen aus dem Vorjahresbericht einzugehen (s. auch den Anhang zu diesem Bericht).

1 Gesamtüberblick

1.1 Entwicklung des Datenschutzes in der Praxis

In den vergangenen fünf Jahren ist der Begriff „Datenschutz" populär geworden, und die Ziele des Gesetzgebers sind in wesentlichen Beziehungen erreicht worden. Doch ist dies kein Zustand, der, einmal erreicht, auf Dauer gesichert wäre; die Umsetzung der gesetzlichen Vorschriften in die Praxis bleibt eine ständige Aufgabe. Zunehmend ist auch die Kritik am Datenschutz gewachsen, und es war nötig, gegen viele Mißverständnisse anzugehen und Unklarheiten auszuräumen. „Skandalöse" Verletzungen der Datenschutzbestimmungen, also vorsätzliche Mißachtung der gesetzlichen Gebote etwa zur persönlichen Bereicherung oder aus Machtmißbrauch sind kaum bekanntgeworden. Gleichwohl hatte ich zahlreiche Datenverarbeitungsvorgänge zu beanstanden, weil sie mit datenschutzrechtlichen Bestimmungen unvereinbar waren. Die verantwortlichen Stellen selbst vertraten oft eine andere Gesetzesauslegung; zumindest waren sich die Handelnden meist nicht bewußt, daß sie anders hätten handeln müssen.

Manche schließen aus solchen Feststellungen, daß das Datenschutzrecht selbst und seine weitere Verbesserung eher unwichtig seien — diese Einschätzung ist so falsch, wie wenn man Strafvorschriften gegen unbefugtes Abhören für überflüssig hielte, weil nur wenige Verstöße dagegen publik geworden seien. Es ist schon nicht auszuschließen, daß den Kontrollinstanzen manche Vorkommnisse unbekannt bleiben. Wenn aber die Zahl der Datenschutzverstöße tatsächlich bisher gering ist, dann kann dies gerade auch eine *Folge* der Datenschutzgesetzgebung und -aufsicht sein. Wir wissen erst wenig über die Wirkungen von Recht und Kontrolle, aber sicher ist, daß *ohne* rechtliche Einschränkungen und *ohne* kontrollierende Instanzen die Hemmschwellen für Fehlverhalten generell niedriger wären.

Den Datenschutzbeauftragten geht es ähnlich wie den Brandschutz-Verantwortlichen: je sicherer die Vorsorge ist, desto weniger Aufmerksamkeit finden ihre weiteren Mahnungen; Erfolg kann zum Hindernis werden. Außerdem erweist sich der Vorteil, daß die Datenschutzgesetzgebung eine relativ *frühe* Reaktion auf technische Neuerungen darstellt und daß sie auch Risiken bekämpft, die sich erst selten realisiert haben, in gewisser Weise als Nachteil für ihre Durchsetzung: das Gesetz ist dem Bewußtsein mancher Interpreten und Anwender vorausgeeilt, und es hat einige der negativen Folgen im Keim erstickt, die eine anderes gewohnte Öffentlichkeit als Beleg seiner Notwendigkeit erwartet.

1.2 Kontroversen

Im vergangenen Jahr sind verschiedene scharf kritische Kommentare zu meiner Tätigkeit veröffentlicht worden. So hat Generalbundesanwalt Prof. Dr. Rebmann einen Artikel mit dem Titel „Sicherheit vor Datenschutz — nicht umgekehrt" verfaßt („Kriminalistik" Heft 3/1982 S. 153f.) und in einem internen Schreiben an den Bundesminister der Justiz, das auszugsweise in einer Tageszeitung abgedruckt wurde, Vorwürfe gegen mich erhoben. Ich habe auf den erwähnten Artikel unter der Überschrift „Sicherheit *und* Datenschutz — keine Alternative" („Kriminalistik" Heft 4/1982 S. 226f.) geantwortet und zu den in der Presse mitgeteilten Ansichten in einem Interview mit dem Berliner Anwaltsblatt (Heft 8/1982 S. 170, 172f.) Stellung genommen. Die CDU/CSU-Fraktion im Deutschen Bundestag hat in einer Kleinen Anfrage (Drucksache 9/1812) auf die Publikationen über das Schreiben des Generalbundesanwalts Bezug genommen; die Bundesregierung hat daraufhin erklärt (Drucksache 9/1889 S. 9), sie habe sich die gegen mich erhobenen Vorwürfe nicht zu eigen gemacht.

Solche Vorgänge werden von der Bevölkerung als „Kontroversen um den Datenschutz" wahrgenommen. Auch unbegründete Attacken bleiben im Gedächtnis haften; die Erwiderung findet meist weniger Echo als der erste Angriff — zumal wenn sie

sachlicher gehalten ist. Ich habe mich — trotz Kenntnis dieser Zusammenhänge — stets darauf beschränkt, Kritikern Sachargumente entgegenzuhalten, selbst wenn sie ihrerseits beleidigende Formulierungen gewählt hatten. Ich habe auch immer wieder das persönliche Gespräch gesucht, in manchen Fällen leider ohne Erfolg.

Ich halte es nicht für angebracht, die Auseinandersetzungen hier fortzuführen. Die Vorwürfe beruhen zum Teil schon auf falschem Verständnis klarer und differenzierter Äußerungen in meinen Berichten. Manche Kritiker haben die Berichte offensichtlich gar nicht gelesen, sonst hätten sie meine Ansichten nicht so falsch zitieren können, wie es bisweilen geschehen ist. Im übrigen war und bin ich durch Geheimhaltungsrücksichten gehindert, meine datenschutzrechtlichen Bewertungen im Bereich der Sicherheitsbehörden in den Tätigkeitsberichten im einzelnen umfassend zu belegen — die Berichte würden dabei auch zu umfangreich. Deshalb mußte ich mich z. B. im Vierten Tätigkeitsbereich (insbesondere S. 21 ff.) auf sehr allgemeine Feststellungen beschränken. Ich habe aber die Belege für diese Einschätzungen in vertraulicher Sitzung des Innenausschusses Punkt für Punkt vorgetragen. Danach hat dort niemand mehr die Richtigkeit meiner tatsächlichen Feststellungen in Zweifel gezogen. Inzwischen hat der Bundesminister des Innern mir auch bestätigt, daß die beanstandeten Maßnahmen der Datenverarbeitung — von wenigen noch ungeklärten oder weiterer Abstimmung bedürftigen Fällen abgesehen — korrigiert worden sind, zuletzt im November 1982 in bezug auf das System PIOS-Terrorismus des Bundeskriminalamtes, einen Hauptgegenstand der vorjährigen Beanstandungen. Weitere Einzelheiten dazu enthält die bereits erwähnte Antwort der Bundesregierung auf die Kleine Anfrage der CDU/CSU-Fraktion (Drucksache 9/1889). Der Innenausschuß hat es in einer Beschlußempfehlung an das Plenum des Deutschen Bundestages (Drucksache 9/2272) begrüßt, daß die Bundesregierung die Bereinigung der beanstandeten Speicherungen mit Nachdruck betreibt.

Manche Vertreter der kontrollierten Stellen hatten erwartet, ich würde die Fortschritte in ihrem Bereich — über das hinaus, was im Vierten Tätigkeitsbericht gesagt ist — stärker herausstellen. Meine Aufgabe ist es aber gerade, die Schwachstellen aufzuzeigen. Von begründeter Kritik kann ich nicht deswegen absehen, weil in *anderer* Hinsicht Anerkennenswertes geleistet wurde. Damit säe ich nicht — wie manche behaupten — Mißtrauen gegen die Sicherheitsbehörden, sondern im Gegenteil: durch genaue Darstellung (und Eingrenzung) dessen, was rechtlich zu beanstanden ist, bestätige ich auch, daß in anderen geprüften Bereichen *kein* Grund zur Beanstandung gegeben war. Pauschalen Behauptungen, die Bundesrepublik sei ein „Überwachungsstaat", bin ich im übrigen bereits vor Jahren entgegengetreten (vgl. z. B. 2. TB S. 4, aber auch zahlreiche Presseäußerungen u. dgl.). Auch dieser Bericht enthält wieder entsprechende Darlegungen. Entgegen stets wiederholten Fehlzitaten habe ich die polizeiliche Methode der „Rasterfahndung" nicht generell verworfen, sondern — in Übereinstimmung mit meinen Kollegen in den Ländern — auf konkrete Rahmenbedingungen und den Regelungsbedarf hingewiesen (3. TB S. 50 f.). Die Antwort der Bundesregierung war freilich äußerst enttäuschend (4. TB S. 52).

Manche Sicherheitsbehörden erwarten nach meinem Eindruck aus nunmehr fast fünf Jahren Prüfungs- und Beratungspraxis von der Kontrollinstanz anscheinend die Bestätigung, daß sie sich stets und überall „hundertprozentig" rechtmäßig verhalten — eine irreale Erwartung, denn keine Behörde kann ständig in sämtlichen Arbeitszusammenhängen rechtmäßig handeln, selbst bei bestem Willen der Leitung und aller Mitarbeiter nicht.

Niemand kommt auf den Gedanken, verwaltungsgerichtliche Urteile, in denen polizeiliche oder nachrichtendienstliche Maßnahmen wegen Rechtswidrigkeit aufgehoben werden, für einen Ausdruck von Mißtrauen zu halten; ebenso wenig gilt dies für Anordnungen der Dienst- oder Fachaufsichtsbehörden. Mir ist auch nicht bekannt, daß parlamentarische Anfragen oder Bemerkungen der Rechnungshöfe als unangebracht bezeichnet worden wären. Die Empfindlichkeit, mit der auf Äußerungen des Datenschutzbeauftragten reagiert wird, ist daher kaum verständlich. Sie ist geeignet, genau das Gegenteil des Gewollten zu bewirken. Durch Bekräftigungsformeln — von welcher Seite auch immer — ist nicht hinwegzureden, daß viele Bürger der Polizei, die das staatliche Gewaltmonopol ausübt, und den Nachrichtendiensten mit Skepsis und zum Teil erheblichem Mißtrauen gegenüberstehen — allein der Umstand, daß diese Stellen vielfach geheim arbeiten, wird immer wieder Unbehagen bei vielen verursachen. Vertrauen kann man nicht durch Worte gewinnen, sondern nur durch Handlungen, und der Appell an die Bürger, sie möchten an die Rechtmäßigkeit staatlicher Maßnahmen glauben, verliert an Überzeugungskraft, wenn gleichzeitig an denjenigen, der die Rechtmäßigkeit unabhängig beurteilen, also eine wesentliche Grundlage für das erwünschte Vertrauen schaffen soll, das Ansinnen gestellt wird, er möge eventuelle Kritik nicht zu stark betonen.

„Da ... nirgends festgeschrieben ist, was das Gemeinwohl inhaltlich umfaßt, und weil niemand von vornherein oder gar ein für alle Male ausmachen kann, was zu dessen Aufrechterhaltung an Offenlegung personenbezogener Daten im konkreten Einzelfall erforderlich ist, muß ein tragfähiger Konsens immer wieder neu geschaffen werden. Damit sind aber auch Differenzen und Konflikte fast zwangsläufig vorprogrammiert. Denn die Bestimmung der aktuellen Erfordernisse basiert nicht nur wesentlich auf den aus dem je verschiedenen weltanschaulichen Verstehenshintergrund fließenden Wertprioritäten und Wertpräferenzen, sondern ebenso auf dem jeweiligen Ermessensurteil hinsichtlich der Situation und der ihr am besten entsprechenden Maßnahmen. Deshalb bleibt auch zur Beantwortung der Frage nach dem jeweils notwendigen Ausmaß des EDV-Einsatzes gar kein anderer Weg als der einer argumentativen und fairen Auseinandersetzung mit demokratischen Mitteln" (Antonellus Elsässer,

Verantwortete Daten- und Informationsverarbeitung. Versuch einer ethischen Orientierung, in: Stimmen der Zeit 1982 S. 113ff., 122). Um es mit eigenen Worten zu formulieren: Ich strebe Konflikte nicht an, weiche ihnen aber nicht aus und sehe in ihnen eine Durchgangsstation auf dem Wege zu besserer Erkenntnis und besserer Praxis.

1.3 Beratungs- und Kontrolltätigkeit im Überblick

Beratungs- und Kontrolltätigkeit lassen sich praktisch nicht gegeneinander abgrenzen. Denn jede sinnvolle Beratung setzt die Feststellung des Zustandes und den Vergleich mit den rechtlichen Vorgaben voraus, und jede Kontrolle, d. h. jeder Vergleich der Realität mit der Rechtslage, führt immer dann zu einer Beratung, wenn Änderungen erforderlich oder sinnvoll scheinen.

Ziel dieser Tätigkeiten ist festzustellen, wie weit die speichernden Stellen durch eigene Maßnahmen die Einhaltung der Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz sicherstellen, die speichernden Stellen dabei zu beraten und auf Lücken und erkannte Vollzugsdefizite hinzuweisen.

Als Methode hat es sich bewährt, sowohl die Erhebung der Sachverhalte als auch die Beratung und die Diskussion von Änderungsmöglichkeiten vor Ort durchzuführen. Dadurch ist gewährleistet, daß die Anforderungen des Datenschutzes auf die Praxis der jeweiligen Aufgabenerfüllung bezogen werden. Die Nutzung des Sachverstandes der Sachbearbeiter, der Vorgesetzten, der Organisatoren und der Datenverarbeiter, der so konzentriert nur in der jeweiligen Behörde selbst angetroffen werden kann, sichert, daß keine Lösungen vorgeschlagen werden, die zwar dem Datenschutz dienen, aber die Aufgabenerfüllung beeinträchtigen oder unangemessen behindert oder verteuern. Im Gegensatz zu dieser oft geäußerten Befürchtung zeigte sich, daß häufig eine so erarbeitete datenschutzgerechte Lösung nicht nur zu weniger Datenbewegung, sondern auch zu weniger Arbeitsaufwand als bisher führt.

Der Erfolg dieses Vorgehens hat mich veranlaßt, die Beratungstätigkeit gegenüber den Vorjahren noch zu verstärken. So ist in diesem Jahr mit insgesamt etwa 450 Manntagen für Kontroll- und Beratungsbesuche bei Behörden die Vorjahreszahl um rund 20 % übertroffen worden.

Um die Besuche erfolgreich durchführen zu können, bedarf es der sorgfältigen Vorbereitung, und auch die angebahnten Beratungskontakte und andere Nacharbeiten binden einen wesentlichen Teil der Kapazität meines Amtes.

1.3.1 Auswahlkriterien

Wegen des hohen Arbeitsaufwandes für jeden Kontroll- und Beratungsbesuch und der Vielzahl von Behörden des Bundes muß stets eine Auswahl getroffen werden. Diese orientiert sich primär an der Bedeutung der Datenverarbeitung der einzelnen Stellen für die betroffenen Bürger, also an der Art der gespeicherten Daten und den Aufgaben der Stelle sowie am Umfang der Datenverarbeitung.

Deshalb und auch weil die Betroffenen in diesem Bereich eigene Kontrollrechte kaum geltend machen können, bilden die Sicherheitsbehörden hier den größten Schwerpunkt. Fast die Hälfte aller Besuchs-Arbeitstage wurde dort geleistet. Dabei ist jedoch zu berücksichtigen, daß die Kontroll- und Beratungsbesuche dort zum Teil sehr lange dauern, weil die Vorbereitung nur beschränkt möglich ist und viele Einzelheiten und Verzweigungen nur anhand der tatsächlichen Datenspeicherung und -verwendung beurteilt werden können. Auch die Möglichkeiten, die Datenverarbeitung mit den rechtlichen Vorgaben zu vereinbaren, werden hier besonders sorgfältig diskutiert, damit unter Verbesserungen des Datenschutzes die Wirksamkeit nicht leidet.

Einen vergleichbar großen Schwerpunkt bildet die Kontroll- und Beratungstätigkeit im Aufgabenbereich Soziale Sicherung. Dort sind die Besuche kürzer und der Vor- und Nachbereitungsanteil am Gesamtaufwand entsprechend höher gewesen. Als Auswahlkriterium tritt hier die Möglichkeit hinzu, mit der Beratung einer Stelle zugleich eine Breitenwirkung auf andere, vergleichbare Stellen zu erzielen. Daneben bieten auch Einzelfälle gelegentlich Anlaß zu einem Besuch, z. B. wenn ein Betroffener in einer Eingabe behauptet, daß er aufgrund unzutreffender Datenspeicherung beim Arbeitsamt keine Aussicht auf eine Arbeitsstelle habe. In solchen Sonderfällen werden Besuche gelegentlich auch ohne vorangehende Ankündigung durchgeführt (s. a. unten Nr. 1.5).

Neben diesen großen Bereichen wurden besonders Stellen mit umfangreicher Datenverarbeitung wie z. B. das Kraftfahrt-Bundesamt kontrolliert.

Nachdem sich gezeigt hatte, daß gerade bei kleineren Einrichtungen ein erheblicher Beratungsbedarf besteht, wurden im Berichtsjahr auch verschiedene Stellen aufgesucht, deren Datenverarbeitung nur wenige Bürger, dafür aber besonders sensible Daten betrifft, wie z. B. die Heimkehrerstiftung.

1.3.2 Das Vorgehen bei Kontrollen

Die Kontrollen müssen sich in der Regel auf Stichproben beschränken und sind stets an den Besonderheiten der jeweiligen Behörde orientiert. Meist wird im Rahmen der Vorbereitung ein Aufgabenbereich oder ein bestimmter, wichtiger Arbeitsablauf ausgesucht, der dann vom Anfang bis zum Ende, d. h. vom Posteingang bis zur Archivierung bzw. Vernichtung der Unterlagen, in allen Einzelschritten verfolgt wird. Dabei werden teils einzelne Fälle durchgehend verfolgt, teils werden auch an den einzelnen Stationen jeweils neue Fälle untersucht. Ein wesentlicher Bestandteil ist oft der Vergleich zwischen der Dokumentation eines Verfahrens und den tatsächlich gespeicherten Daten.

Es ist offensichtlich, daß dazu der Einblick in personenbezogene Daten unerläßlich ist. Deshalb sind

Kontrollen in den Bereichen, in denen mir aufgrund besonderer Geheimhaltungsvorschriften die Einsicht in die gespeicherten Daten verwehrt wird, erheblich behindert; siehe dazu auch Nr. 2.3.1 und Nr. 2.5.1 in diesem Bericht. Denn häufig, insbesondere wenn die Dokumentation automatisierter Verfahren Mängel aufweist, ungenau ist oder die Realisierung von der Dokumentation abweicht, liefert nur der Einblick in die Daten selbst eine zuverlässige Information über die Verfahren.

1.3.3 Maßstäbe der Kontrolle

Maßstäbe der Kontrolle sind *Rechtsnormen*, und zwar neben den Bestimmungen des Bundesdatenschutzgesetzes selbst noch zahlreiche andere Vorschriften über den Datenschutz, z. B. §§ 35 SGB I, 67 ff SGB X, das Melderechtsrahmengesetz und Geheimhaltungs-, aber auch Übermittlungsvorschriften in zahlreichen Spezialgesetzen, insbesondere für den Bereich der Statistik, sowie Normen über Berufs- und besondere Amtsgeheimnisse und das ungeschriebene, von der Rechtsprechung entwickelte Recht der Personalaktenführung. Bei der Auslegung und Anwendung der Datenschutzbestimmungen spielen häufig Verfassungsnormen eine Rolle; sie sind dann in den jeweiligen Zusammenhängen zu beachten.

Die Kontrolle der Einhaltung „anderer" Datenschutzvorschriften (außerhalb des BDSG) ist nicht auf die Fälle eingeschränkt, in denen die Daten in Dateien gespeichert oder aus ihnen übermittelt werden (ausführliche Begründung dazu im 3. TB S. 57 f.). Diese Rechtsauffassung wird von den Landesbeauftragten für den Datenschutz für ihren Bereich geteilt (mit der Ausnahme von Schleswig-Holstein, weil der Text des Landesdatenschutzgesetzes — § 1 Abs. 1 — von dem des BDSG und anderer Landesdatenschutzgesetze abweicht).

Der Bundesbeauftragte für den Datenschutz ist in Ausübung seines Amtes „nur dem Gesetz unterworfen" (§ 17 Abs. 4 S. 2 BDSG). Dies bedeutet auch, daß er bei der Auslegung des Gesetzes keinen Weisungen unterworfen ist. Es steht ihm kraft seiner Unabhängigkeit zu, diejenige Auslegung zu vertreten, die nach seiner Einschätzung seinem Auftrag — Schutz von Bürgerrechten — am besten gerecht wird. Solange diese Auslegung nicht gegen den eindeutigen Wortlaut des Gesetzes verstößt, kann sie nicht im Wege der Rechtsaufsicht der Bundesregierung beanstandet werden. Sind zu einer Rechtsfrage mehrere sich widersprechende Auslegungen vertretbar, so kann die Rechtsaufsichtsinstanz nicht ihre „richtige" gegen die angebliche „falsche" Auffassung des BfD setzen. Ein etwaiger Konflikt bedürfte auch keiner ausdrücklichen autoritativen Lösung, weil die Bundesregierung mittels ihrer Weisungsbefugnisse ihre Rechtsauffassung gegen die des BfD bei der Verwaltung durchsetzen kann.

1.3.4 Ergebnisse der Beratungs- und Kontrolltätigkeit

Ein wohl häufig vorkommender und gelegentlich auch auffälliger Effekt meiner Kontrolltätigkeit ist, daß allein die Ankündigung eines Besuchs die Verantwortlichen in der Behörde zu einer Eigenkontrolle veranlaßt. Darüber hinaus führt die enge Zusammenarbeit mit dem jeweils für den Datenschutz Zuständigen oft dazu, daß dieser Schwachstellen zukünftig leichter erkennt und die Möglichkeit, den Datenschutz sicherzustellen, verbessert wird.

Bei fast jedem Besuch wurden Verbesserungsmöglichkeiten oder auch Mängel festgestellt, erhebliche Mängel — die beanstandet werden mußten — jedoch nur bei jeder vierten Prüfung. So führten die insgesamt 31 Kontroll- und Beratungsbesuche in diesem Berichtsjahr nur bei 7 Stellen zu förmlichen Beanstandungen (die freilich zum Teil sehr zahlreich waren und zum Teil größere Komplexe betrafen). Diese und die sonst festgestellten Mängel lagen zu zwei Dritteln im materiell-rechtlichen Bereich; einen wesentlichen Anteil bildeten hier die Fälle zu langer Speicherung, besonders bei den Sicherheitsbehörden. Ein Drittel der Mängel lag in unzureichenden technischen und organisatorischen Maßnahmen zur Datensicherung.

Als Ergebnis der intensiven Beratung ist bei über 80 % der in den vorangegangenen Jahren festgestellten Mängel die Beseitigung erfolgt oder zumindest so eingeleitet, daß eine nachgehende Beratung nicht erforderlich ist. Dies gilt auch für etwas über 50 % der im Berichtsjahr festgestellten Mängel. Die übrigen Fälle sind zum Teil deswegen noch offen, weil keine Einigkeit über die rechtliche Bewertung besteht, zum Teil aber auch deshalb, weil Umstellungen oft schwierig sind und besonders im technisch-organisatorischen Bereich Zeit, gelegentlich aber auch Geld kosten.

Die noch nicht erledigten Beanstandungen und anderen Probleme, die in meinem Vierten Tätigkeitsbericht beschrieben wurden, sind jeweils mit einem Hinweis zur weiteren Entwicklung im Anhang zu diesem Bericht zusammengestellt.

1.4 Kooperation mit anderen Stellen

Die in § 19 Abs. 5 geforderte Kooperation mit den Datenschutzbeauftragten der Länder bzw. der Datenschutzkommission in Rheinland-Pfalz und den Aufsichtsbehörden gemäß §§ 30, 40 BDSG hat sich stets als eine wertvolle Hilfe sowohl bei der Auslegung einzelner Vorschriften als auch bei der Weiterentwicklung des Datenschutzrechts erwiesen.

Die Kontrollinstanzen für den öffentlichen Bereich haben die Zusammenarbeit in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder institutionalisiert, die im Jahre 1982 dreimal getagt hat. Besondere Schwerpunkte der Beratungen waren die Novellierung des BDSG, die Datenverarbeitung in der Finanzverwaltung, Überlegungen zu dem Musterentwurf eines Krebsregistergesetzes und zum Datenschutz bei der wissenschaftlichen Forschung, das Archivwesen und Fragen des Datenschutzes bei den Neuen Medien. Dabei erwies es sich als sehr zweckmäßig, die oft schwierigen und komplexen Probleme in speziellen Arbeitskreisen

vorzuberaten. Als besonders wirksam hat sich auch der Arbeitskreis „Sicherheit“ erwiesen, in dem u. a. das Vorgehen bei der Kontrolle von im Bund-Länder-Verbund arbeitenden Sicherheitsbehörden beraten wurde.

Die für die Datenverarbeitung nicht-öffentlicher Stellen zuständigen Aufsichtsbehörden der Länder stimmen ihr Vorgehen im „Düsseldorfer Kreis“ ab. An den vier Sitzungen des Berichtszeitraums nahmen stets auch Mitarbeiter meiner Dienststelle teil. Dadurch und weil mehrere Landesbeauftragte für den Datenschutz auch die Aufgaben der Aufsichtsbehörden nach §§ 30, 40 BDSG wahrnehmen und deshalb auch im Düsseldorfer Kreis vertreten sind, wird die Abstimmung zwischen den Kontrollinstanzen für den öffentlichen und denen für den nichtöffentlichen Bereich erheblich erleichtert. Wichtige Themen der Beratungen waren einheitliche Grundsätze für die Auslegung des Begriffs „schutzwürdige Belange“, die Übermittlung von Daten aus Unternehmen (z. B. über Mitarbeiter) an Strafverfolgungsbehörden, die Übermittlung von Daten der Kreditauskunfteien durch Direktabruf, die Telefondatenerfassung in Nebenstellenanlagen, die Probleme bei Medienarchiven sowie die Novellierung des BDSG.

Die Zusammenarbeit der für die Kontrolle des Datenschutzes zuständigen Behörden im Bund und in den Ländern hat sich bewährt. Es ist in fast allen Fällen gelungen, Ergebnisse zu finden, die gemeinsam getragen werden konnten. Damit ist zu erwarten, daß die Einheitlichkeit der Auslegung und Anwendung des Datenschutzrechts in allen wesentlichen Punkten auch in Zukunft gewahrt werden kann.

Außer der Beteiligung an den Beratungen der Datenschutz-Kontrollinstanzen habe ich im Berichtsjahr wieder die Möglichkeit wahrgenommen, im Fachausschuß „Datenschutz und Datensicherung“ des Ausschusses für wirtschaftliche Verwaltung in Wirtschaft und öffentlicher Hand e. V. (AWV) und in einigen seiner Projektgruppen mit Vertretern großer DV-Anwender aus der privaten Wirtschaft und Herstellern von DV-Anlagen über Fragen des Datenschutzes zu diskutieren. Auch wenn gerade hier die recht unterschiedliche Interessenlage oft zu Meinungsverschiedenheiten führt, so ist doch das gegenseitige Kennenlernen der Standpunkte nützlich.

Auch in diesem Jahr hat ein Vertreter meiner Dienststelle in der Arbeitsgruppe „Datenschutz“ der Bundesvereinigung der Kommunalen Spitzenverbände, die sich mit der Ausführung der Datenschutzgesetze in den Kommunalverwaltungen beschäftigt, über meine Erfahrungen berichtet und an den Beratungen der Arbeitsgruppe als Gast teilgenommen.

1.5 Meinungsverschiedenheiten mit dem Ausschuß für Organisationsfragen

Die Eigenart meiner gesetzlich festgelegten Aufgaben bedingt zuweilen ungewöhnliches Vorgehen bei ihrer Erfüllung. So haben meine Mitarbeiter einige Kontrollbesuche bei Behörden durchgeführt, ohne sich vorher anzukündigen. Schriftwechsel mit nachgeordneten Behörden der Bundesministerien führe ich ausnahmsweise auch unmittelbar mit jenen, ohne das vorgesetzte Bundesministerium zu beteiligen.

Auf Veranlassung einiger Bundesministerien, die insbesondere einen angeblichen Verstoß gegen § 71 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO I) rügten, hat sich der Ausschuß für Organisationsfragen (AfO, § 9 GGO I) mit diesem Verfahren befaßt. Die Bundesressorts betonten die Notwendigkeit einer engeren vertrauensvollen Zusammenarbeit, baten um Unterrichtung auch in Routineangelegenheiten, sofern ein beanstandeter Sachverhalt erstmalig auftritt, ferner um Unterrichtung über positive wie negative Prüfungsergebnisse, um in die Lage versetzt zu werden, die Fachaufsicht ergebnisorientiert auszuüben, rechtzeitig reagieren und gegebenenfalls präventiv gestaltend einwirken zu können; als weiteres Anliegen wurde eine einheitliche Handhabung des Besuchs- und Schriftverkehrs mit nachgeordneten Behörden hervorgehoben. Auf Wunsch eines Bundesressorts, das gleichzeitig volle Zufriedenheit über die von mir geübte Praxis des Schrift- und Besuchsverkehrs betonte, beauftragte der AfO den Bundesminister des Innern, eine gutachtliche Stellungnahme über den „Geschäftsverkehr des BfD mit den obersten Bundesbehörden und deren nachgeordneten Dienststellen“ anzufertigen.

Diese Stellungnahme, die vom AfO zustimmend zur Kenntnis genommen wurde, hat im wesentlichen folgenden Inhalt:

Ausgehend von § 71 Abs. 1 Satz 1 GGO I, wonach die Ministerien außerhalb ihres eigenen Geschäftsbereichs regelmäßig nur mit den obersten Bundesbehörden verkehren, sei festzustellen, daß nachgeordneten Behörden Besuche nur nach vorheriger Anmeldung bei der zuständigen obersten Bundesbehörde abgestattet werden könnten. Denn das BDSG enthalte — anders als das Gesetz über den Wehrbeauftragten und einige Landesdatenschutzgesetze — keine ausdrückliche Befugnis zu unangemeldeten Besuchen. Auch hinsichtlich des Schriftverkehrs sei im BDSG keine Vorschrift ersichtlich, die als Ausnahmeregelung zu § 71 Abs. 1 Satz 1 GGO I gelten könne.

Ich habe demgegenüber erklärt, daß ich aus meiner gesetzlichen Kontrollaufgabe, die sich auf alle Behörden der Bundesverwaltung erstreckt, insbesondere aus der gesetzlichen Verpflichtung dieser Behörden, mir Auskunft zu meinen Fragen, Einsicht in alle mit der Datenverarbeitung zusammenhängenden Unterlagen und Akten sowie *jederzeit* Zutritt in alle Diensträume zu gewähren (§ 19 Abs. 1 und Abs. 3 Satz 2 Nr. 1 und 2 BDSG), die Befugnis ableite, auch unangemeldet Behörden des nachgeordneten Bereichs aufzusuchen und mit diesen unmittelbar zu korrespondieren. Die GGO I, die lediglich den Rang einer Verwaltungsvorschrift besitzt, kann diese gesetzlichen Regelungen nicht verdrängen. Die in Frage stehenden Befugnisse sind unab-

dingbar, um meine Kontrolltätigkeit effektiv ausüben zu können, und sind Folge meiner Unabhängigkeit. Gleichwohl mache ich davon nur äußerst sparsamen Gebrauch. Nur in wenigen Fällen, in denen Eingaben von Betroffenen dazu Anlaß gaben, habe ich Behörden unangemeldet aufgesucht, um „beschönigende" Vorkehrungen zu verhindern. Schriftwechsel führe ich ebenfalls nur in Ausnahmefällen ohne Beteiligung der obersten Bundesbehörde, nämlich dann, wenn die Kenntnisnahme eines größeren Empfängerkreises schutzwürdige Belange bestimmter Betroffener beeinträchtigen könnte. Mit einigen obersten Bundesbehörden bestehen wegen spezifischer Gegebenheiten Absprachen darüber, daß ich nur die oberste Bundesbehörde anschreibe (Bundeskanzleramt, Bundesminister der Verteidigung, Bundesminister für das Post- und Fernmeldewesen) oder insbesondere in Routine- oder Bagatellfällen unmittelbar mit der betreffenden Behörde korrespondiere. In aller Regel erhalten die obersten Bundesbehörden nachrichtlich Abdrucke meiner Schreiben oder diese werden über die oberste Bundesbehörde geleitet. Dieses Verfahren hat sich bewährt; ich sehe keinen Anlaß davon abzugehen. Die vom AfO gewünschte Zusammenarbeit und Unterrichtung über sämtliche Prüfungsergebnisse wird praktiziert. Im übrigen ist es jeder obersten Bundesbehörde unbenommen, im Wege der Fachaufsicht über die nachgeordneten Dienststellen diese zu umfassender Berichterstattung anzuweisen.

1.6 Öffentlichkeitsarbeit

Das Interesse an Informationen über den Datenschutz ist unverändert groß. Zur Beantwortung der allgemein gehaltenen Anfragen verwende ich dabei zwei Broschüren, die ich auf Wunsch zusende, und zwar kostenlos:

— „Bürgerfibel Datenschutz"

  In dieser Broschüre, die auch den Text des BDSG enthält, sind die für den Bürger wichtigsten Datenschutzvorschriften erläutert. Sie wurde im Jahre 1980 als überarbeitete Fassung der bereits 1978 erschienenen Schrift „Was bringt das Datenschutzgesetz?" herausgegeben.

— „Der Bürger und seine Daten"

  Diese Broschüre wurde von mir gemeinsam mit anderen Datenschutz-Kontrollinstanzen entwikkelt. Sie enthält eine Beschreibung wichtiger und häufig vorkommender Datenspeicherungen, mit denen ein Bürger bei seinen Kontakten mit Behörden und privaten Stellen rechnen muß.

Von jeder dieser Broschüren habe ich bisher etwa 150 000 Exemplare versandt, davon im Jahre 1982 etwa je 40 000. Beide Broschüren werden in erheblichem Umfang von einzelnen Bürgern angefordert, überwiegend aber von Betrieben, Vereinigungen und Verbänden sowie von Schulen und anderen Bildungseinrichtungen.

In Vorbereitung befindet sich eine Broschüre über Datenverarbeitung und Datenschutz bei den Sozialleistungsträgern (Sozialdaten-Fibel).

Ähnlich wie in den vorangegangenen Jahren habe ich von meinem Vierten Tätigkeitsbericht ca. 4 000 Exemplare versandt. Die Nachfrage nach meinen Tätigkeitsberichten kommt überwiegend aus der Fachöffentlichkeit, besonders von öffentlichen und privaten Stellen, die Daten verarbeiten, und von interessierten Journalisten, in letzter Zeit zunehmend auch von Studenten der entsprechenden Fachrichtungen.

Außer mit der Presseerklärung zur Vorstellung meines Vierten Tätigkeitsberichtes habe ich mit vier weiteren Mitteilungen zu einzelnen Diskussionsthemen Stellung genommen.

Eine dieser Erklärungen betraf u. a. irreführende Pressemeldungen über die Verwendung von Sozialdaten. Eine weitere beschäftigte sich mit den vom Generalbundesanwalt veröffentlichten Überlegungen zum Datenschutz bei den Sicherheitsbehörden, die dritte Pressemitteilung behandelte das Verhältnis zwischen Forschung und Datenschutz und die vierte trat unzutreffenden Meldungen über die Einschränkung meiner Kontrollbefugnisse entgegen. Zu diesen, aber auch zu anderen Fragen des Datenschutzes habe ich zahlreiche Interviews gegeben, und die Reaktionen daruf zeigen, daß es die Bürger durchaus interessiert, was mit ihren Daten geschieht oder geschehen könnte und wie wirksam der Datenschutz ist.

Wie auch in den vorigen Jahren haben meine Mitarbeiter und ich auch an mehreren Tagungen und Seminaren mitgewirkt, bei denen teils die Anwendung, teils die Fortentwicklung des Datenschutzrechts im Vordergrund standen oder im Rahmen einer anderen Problematik besondere Bedeutung hatten.

1.7 Dateienregister und Veröffentlichungen über Dateien

Zu dem in meiner Dienststelle geführten Register der von öffentlichen Stellen des Bundes automatisch betriebenen Dateien mit personenbezogenen Daten sind zur Zeit etwa 1 200 Dateien gemeldet. Das Wachstum dieses Dateienregisters um jährlich etwa 100 Meldungen beruht nicht nur auf einer Zunahme der automatisierten Datenverarbeitung, sondern auch darauf, daß noch immer Nachmeldungen eintreffen und alte Meldungen präzisiert und dabei mehr Dateien gemeldet werden.

Auch in diesem Berichtszeitraum haben nur sehr wenige Bürger von ihrem Recht Gebrauch gemacht, das Register einzusehen. Die Einsicht in das Register ist im Normalfall auch wenig hilfreich, denn die Meldungen liefern für den Bürger in der Regel weder ein vollständiges noch ein verständliches Bild der Datenverarbeitung einer einzelnen Stelle, geschweige denn der Gesamtheit der öffentlichen Stellen des Bundes oder gar einen Ansatz zur Lösung eines individuellen Problems. Der — begrenzte — Wert des Registers liegt vielmehr darin, daß ich daraus einen ersten Überblick über die Datenverarbeitung der einzelnen Stellen bekomme so-

wie darüber, wie die Stelle zumindest diese Formalpflicht nach dem BDSG erfüllt. Darüber hinaus erfahre ich dadurch auch von neu angelegten Dateien.

Weit weniger sinnvoll scheinen mir die Veröffentlichungen im Bundesanzeiger zu sein. Abgesehen davon, daß durch Ausnahmen von der Veröffentlichungspflicht das gezeigte Bild der Datenverarbeitung lückenhaft bleibt, ist es auch durch die Verteilung auf nunmehr 17 Bekanntmachungen, in denen zum Teil Ergänzungen und Änderungen, zum Teil auch Auflösungen von Dateien angezeigt werden, extrem unübersichtlich geworden. Auch das Sachregister, das jährlich aktualisiert wird, hilft dem Bürger bei der Suche, welche Stellen Daten über ihn gespeichert haben könnten, nur wenig. So kommen z. B. Stichworte wie „Bußgeld“, „Ordnungswidrigkeit“ oder gar „Straftaten“ im Sachregister nicht vor, wohl aber Hinweise auf etwa je 15 Autorenkarteien und Bibliothekskataloge. Die mit weiteren Ergänzungen zunehmende Nutzlosigkeit dieser Veröffentlichungen sollte bald Anlaß zu einer grundlegenden Änderung sein (s. unten Nr. 6.2).

1.8 Die Dienststelle

Der Aufbau meiner Dienststelle hat sich in den ersten Jahren meiner Amtszeit in personeller, organisatorischer und haushaltsmäßiger Hinsicht kontinuierlich vollzogen. Bei meinem Amtsantritt fand ich zunächst nur wenige Mitarbeiter vor, die mir der Bundesminister des Innern zur Seite gestellt hatte. Nach ratenweiser Erhöhung des Stellenplans wies der Bundeshaushalt 1980 erstmalig den heutigen Personalstand von zwanzig Beamten, sieben Angestellten und zwei Arbeitern aus. Von meinen beamteten Mitarbeitern gehören zwölf dem höheren, sechs dem gehobenen und einer dem mittleren Dienst an. Eine im Interesse einer noch wirksameren vorbeugenden Beratung der Bundesbehörden in Datenschutzfragen wünschenswerte Aufstokkung um je einen Beamten des höheren und des gehobenen Dienstes war wegen der schlechten Haushaltslage des Bundes nicht möglich. Ich habe darauf auch nicht nachdrücklich bestanden, weil die Dienststelle mit der gegenwärtigen Personalausstattung zumindest ihren Kontrollauftrag zufriedenstellend erfüllen konnte.

Es war nicht leicht, das für die spezifischen Aufgaben der Dienststelle geeignete Personal zu gewinnen. Die Besetzung einiger Stellen erfolgte erst aufgrund von Ausschreibungen und nach langwierigen Auswahlverfahren, die zunächst Entscheidungen über die zu fordernde Qualifikation der Bewerber voraussetzten. Schon erste Überlegungen machten deutlich, daß neben juristisch vorgebildeten Mitarbeitern auch solche mit Qualifikation in der Datenverarbeitung und mit organisatorischer Befähigung benötigt wurden. Insbesondere in der Anlaufzeit meiner Tätigkeit kam es darauf an, viele zentrale Rechtsfragen, die sich bei Anwendung und Auslegung des komplizierten Gesetzestextes stellten, zu klären, zumal sich die Literatur zum Datenschutzrecht erst allmählich entwickelte und „herrschende Meinungen“ sich nur in mühsamen Abstimmungsprozessen herausbildeten. Bei Kontrollbesuchen vor allem bei Behörden, die mit Datenverarbeitungsanlagen ausgestattet sind, erwies sich die Beteiligung von Fachkräften der Datenverarbeitung und der Organisation als nützlich, teils als unentbehrlich. Die derzeitige Zusammensetzung der Beamtenschaft meiner Dienststelle, in der im höheren Dienst neben Juristen auch drei Nichtjuristen der Fachrichtungen Mathematik, Nachrichtentechnik und Wirtschaftswissenschaften tätig sind und alle Angehörigen des gehobenen Dienstes über praktische Erfahrungen und besondere Ausbildungen in der automatisierten Datenverarbeitung und in der Organisation verfügen, entspricht den Bedürfnissen und hat sich bewährt. Bei der Auswahl des Personals, die der Bundesminister des Innern in allen Fällen mit meinem Einvernehmen vorgenommen hat, habe ich auf technisches Verständnis, Bereitschaft zu permanenter Fortbildung und Interesse und Engagement für Datenschutz besonderen Wert gelegt. Ich muß an dieser Stelle jedoch einem verbreiteten Irrtum entgegentreten: Die Arbeit in meiner Dienststelle erfordert nicht den Spezialisten und bringt ihn auch nicht hervor. Die Klärung datenschutzrechtlicher Probleme verlangt nicht anders als in den meisten Arbeitsbereichen der Ministerialverwaltung auch die Kenntnis allgemeiner Rechtsbegriffe und Anwendungsmethoden. Die datenschutzrechtliche Bewertung von Verwaltungsvorgängen hat sich stets an den Erfordernissen rechtmäßiger Aufgabenerfüllung zu orientieren und setzt deshalb voraus, daß sich derjenige, der Kontrolle ausübt, mit den Aufgaben der kontrollierten Behörde, den bei ihrer Wahrnehmung zu beachtenden Rechtsvorschriften und den jeweiligen Verfahrensabläufen vertraut macht. Dies hat zur Folge, daß meine Mitarbeiter im Laufe ihrer Tätigkeit zunehmendes Wissen über zahlreiche, sehr verschiedene Verwaltungszweige erlangt und auf vielen Rechtsgebieten beachtliche Fachkompetenz erworben haben. Nur so konnte die Beratungsaufgabe meiner Dienststelle wirksam erfüllt werden. Datenschutz ist eine Querschnittsmaterie, die es ermöglicht, aber auch dazu zwingt, sich intensiv mit aufgabenspezifischem Recht und den bei seiner Anwendung zu beachtenden Fachfragen auseinanderzusetzen. Ich treffe diese Feststellung auch im Interesse meiner Mitarbeiter, deren berufliche Entwicklungsmöglichkeiten nicht durch die irrige Vermutung, es handele sich um nur beschränkt einsetzbare Spezialisten, verbaut werden sollten.

Die organisatorische Gliederung der Dienststelle habe ich der der Ministerialverwaltung angepaßt, indem fünf Referate gebildet wurden, die — abgesehen von einem Grundsatzreferat und der Konzentration einiger übergreifender Querschnittsaufgaben — jeweils für bestimmte Arbeitsbereiche der Bundesressorts zuständig sind. Die Zuständigkeitsverteilung folgte einmal dem Prinzip, ähnliche Ressortaufgaben jeweils zusammenzufassen, zum anderen der Rücksichtnahme auf Vortätigkeiten, Erfahrungen und Interessen der Mitarbeiter. Diese Organisationsstruktur, die durch gegenseitige fachliche Beteiligung flexibel gehalten wird, hat sich bewährt.

Das Haushaltsvolumen meiner Dienststelle, das in einem besonderen Kapitel des Einzelplans des Bundesministers des Innern veranschlagt wird, betrug im Jahre 1982 2,279 Mio. DM mit einem Anteil der Personalausgaben von 1,772 Mio. DM. Der Gesamthaushalt meines Amtes entspricht etwa einem Drittel dessen, was das Bundesgesundheitsamt allein für seine Datenverarbeitung ausgibt, und etwa zwei Dritteln des Haushalts des Wehrbeauftragten des Deutschen Bundestages. Ich bin mir der Fragwürdigkeit solcher Vergleichsrechnungen durchaus bewußt; gleichwohl mögen sie deutlich machen, daß es abwegig ist, die Datenschutzkontrolle in der Bundesverwaltung als aufwendige „Datenschutzbürokratie" zu bezeichnen. Ein „teures Spielzeug" — wie ein Journalist meinte — ist sie erst recht nicht. *Ganz umsonst* ist auch Grundrechtsschutz nicht zu haben (s. a. sogleich 1.9).

1.9 Kosten des Datenschutzes

Vergleicht man die Zahl der Mitarbeiter in meiner Dienststelle (30) mit der Zahl der Mitarbeiter bei Bundesministerien (ca. 20 000) oder gar der Zahl der Bundesbediensteten (ohne Bahn, ohne Post und ohne Soldaten ca. 300 000) so ist klar, daß die Datenschutz-„Bürokratie" keineswegs überdimensioniert ist. Bei den großen Datenverarbeitern des Bundes sind sicher jeweils zehnmal mehr Personen mit der Datenverarbeitung beschäftigt, als insgesamt für alle Bundesbehörden zur Kontrolle eingesetzt werden. Daß eine wirksame Datenschutz-Kontrolle auch nicht besonders teuer sein muß, zeigt ein Vergleich der Haushaltsansätze:

Der Haushalt meiner Dienststelle in Höhe von rd. 2,3 Mio. DM (siehe auch oben Nr. 1.8) hat am Haushalt des BMI einen Anteil von etwa 0,07 %, er liegt damit noch etwas niedriger als z. B. die Ausgaben für Heizung, Beleuchtung und sonstigen Energiebedarf allein für den Deutschen Wetterdienst in Offenbach (Main).

Schwieriger, als es diese direkten Kostenvergleiche zeigen, ist eine Abschätzung der Folgekosten des Datenschutzes in den Behörden. Hier fällt zunächst auf, daß manche organisatorischen und technischen Maßnahmen der Datensicherung offensichtlich Kosten verursachen, denen Einsparungen oder ein anderer unmittelbar erkennbarer Nutzen nicht gegenüberstehen. Dies gilt z. B., wenn wegen der Art der Daten oder der großen Zahl der Betroffenen für den Versand von Datenträgern besondere Versandarten wie z. B. Wertbrief angemessen erscheinen, was den häufig knapp bemessenen Haushaltsansatz für Telefon und Porto belasten würde. Und es gilt seltener, dann aber mit größeren Beträgen, wenn zur Sicherung der Daten bauliche Maßnahmen erforderlich sind. Nicht immer sind solche Maßnahmen allein schon wegen des Schutzes der Sachwerte gerechtfertigt. Wenn die Behörden aber ihre Treuhänderschaft für die Daten, die ihnen von den Bürgern im Vertrauen auf die sorgfältige Behandlung offenbart werden oder werden müssen, ernst nehmen sollen, dann muß akzeptiert werden, daß einige der erforderlichen Sicherungsmaßnahmen auch Kosten verursachen.

Als eine weitere Ursache für Folgekosten des Datenschutzes ist zu berücksichtigen, daß bei den Behörden, die sich bemüht haben, die gesetzlichen Anforderungen voll zu erfüllen, zunächst eine gewisse Unruhe entstand und insbesondere die Erfassung aller Dateien mit personenbezogenen Daten in der nach § 15 BDSG vorgeschriebenen Übersicht, die Meldungen zum Register nach § 19 Abs. 4 und die Vorbereitung der Veröffentlichung gemäß § 12 BDSG häufig viel Mühe bereiteten. Dieser Eindruck relativiert sich, wenn man bedenkt, welchen Aufwand die Einrichtung oder Änderung einer Datei und die Einfügung dieser Maßnahmen in die Arbeitsorganisation einer Behörde erfordern. Verglichen damit ist der Aufwand für die Erfüllung der Formalpflichten nach dem BDSG verschwindend gering.

Außerdem war der gesetzliche Zwang, eine Übersicht anzulegen, auch sehr hilfreich, die zum Teil etwas chaotisch gewachsenen Strukturen zu durchleuchten und zu durchforsten. So war z. B. der Bundesminister der Verteidigung äußerst erfolgreich mit seinen Bemühungen, die Erfassung aller Dateien zu einer tiefgreifenden Bereinigung zu nutzen, die zu Vereinfachungen und damit zu Kosteneinsparungen führt.

Effekte dieser Art bewirkt das BDSG, weil es die erste weitgehend umfassende rechtliche Vorgabe für die Datenverarbeitung der Behörden darstellt. Implizit setzt es dabei geordnete Verhältnisse voraus, die aber selbst bei der automatisierten Datenverarbeitung, die sowohl hinsichtlich der Datenverarbeitungsanlagen als auch bei den Programmen in den letzten drei Jahrzehnten bis zu vier Generationen erlebt hat, keineswegs immer vorgelegen haben. Außerdem sieht das BDSG die Technik — und damit auch die EDV-Abteilungen der Behörden — in einer dienenden Funktion, deren Leistung von den rechtlichen und fachlichen Vorgaben bestimmt wird, und unterstellt damit Verhältnisse, die häufig nicht gegeben sind. Wo es besonderer Anstrengungen bedarf, diese Verhältnisse wegen oder mit Hilfe des BDSG zurechtzurücken, ist man leicht geneigt, sämtliche dabei anfallenden Kosten dem Datenschutz zuzurechnen, und berücksichtigt nicht die Vorteile sachgerechter, überschaubarer und beherrschbarer Strukturen.

Damit wird deutlich, daß die Kostenwirkungen des Bundesdatenschutzgesetzes zwar praktisch nicht berechenbar, mit Sicherheit aber nicht hoch sind.

Daß diese Einschätzung auch von unabhängigen Fachleuten geteilt wird, zeigen z. B. die Äußerungen des Vertreters des Bundesrechnungshofs in der Sitzung des Interministeriellen Ausschusses zur Koordinierung der Datenverarbeitung in der Bundesverwaltung am 4. März 1982, wonach Datenschutzerfordernisse zwar den Begriff der Wirtschaftlichkeit relativieren könnten, bisher aber, soweit bekannt,

nicht zu objektiv unwirtschaftlichen Lösungen geführt hätten.

Bei diesen Überlegungen zu den Kostenwirkungen des Datenschutzes ist ein besonderer Effekt nicht berücksichtigt, der sich im Laufe meiner Tätigkeit gezeigt hat. Bei der intensiven Beratung zahlreicher Stellen sind in meiner Dienststelle beinahe beiläufig vielfältige Kenntnisse über den Stand und eine angemessene Organisation der Datenverarbeitung in der öffentlichen Verwaltung entstanden. Durch die Weitergabe dieses Wissens war es möglich, zur zweckmäßigen und kostensparenden Regelung von Verwaltungsaufgaben beizutragen, die nur durch die sinnvolle Zusammenarbeit unterschiedlicher Stellen zu bewältigen sind (siehe dazu Nr. 2.1.1 in diesem Bericht).

1.10 Eingaben

Im Berichtsjahr erreichten mich ca. 1000 schriftliche Bürgereingaben. Nicht darin enthalten sind Anforderungen von Informationsmaterial und einfache Anfragen, die sich durch Hinweise auf gleichzeitig übersandte Informationsschriften beantworten ließen. Die in den Eingaben vorgebrachten Anliegen waren sehr unterschiedlich; sie betrafen überwiegend die Bereiche soziale Sicherung, öffentliche Sicherheit und die Post. In vielen Fällen konnte ich für Abhilfe sorgen oder Ratschläge geben. Häufig konnte ich auch durch eine Erläuterung der Zusammenhänge unberechtigtes Mißtrauen gegenüber der öffentlichen Verwaltung abbauen und Verständnis für deren Maßnahmen schaffen. Näheres zu den wichtigsten Eingaben wird im jeweiligen Sachzusammenhang berichtet.

2 Feststellungen aus der Kontroll- und Beratungstätigkeit in den verschiedenen Bereichen der Bundesverwaltung

2.1 Allgemeine innere Verwaltung

2.1.1 Melderecht

Die zeitgemäße Neuordnung des Meldewesens durch Bundesrahmenrecht und die Entwicklung des Datenschutzrechts haben eine langjährige gemeinsame Geschichte. Vor allem der Plan, mit einem Bundesmeldegesetz ein bundeseinheitliches Personenkennzeichen für jeden Bürger einzuführen, gab den Anstoß für erste Überlegungen zu einer gesetzlichen Regelung des Persönlichkeitsschutzes und hat schließlich die Verabschiedung des Bundesdatenschutzgesetzes stark forciert. Denn der Entwurf eines Bundesmeldegesetzes und der wenig später vorgelegte Entwurf des Bundesdatenschutzgesetzes wurden vom Parlament durch ein Junktim aneinander gebunden: ein Bundesmeldegesetz sollte nur verabschiedet werden, wenn gleichzeitig eine wirksame Regelung des Datenschutzes geschaffen würde.

Der Entwurf eines Bundesmeldegesetzes scheiterte später an einem Votum des Rechtsausschusses des Deutschen Bundestages, der in seiner Stellungnahme vom 5. Mai 1976 zum Entwurf eines Bundesdatenschutzgesetzes u. a. ausführte, daß die Entwicklung, Einführung und Verwendung eines Personenkennzeichens unzulässig sei. Maßgebend dafür waren verfassungsrechtliche Bedenken.

Nach Verabschiedung des Bundesdatenschutzgesetzes und Einrichtung meiner Dienststelle war es eine meiner ersten Aufgaben, ein Gutachten zum Melderecht für den Bundesminister des Innern zu erstellen (s. 1. TB S. 13 f. und 2. TB S. 13 f.). Dieses Gutachten vom 15. Oktober 1978 und die Ergebnisse der Sachverständigenanhörung vom 20./21. November 1978 haben maßgeblich den Entwurf eines Melderechtsrahmengesetzes der Bundesregierung geprägt. Das Melderechtsrahmengesetz (MRRG) wurde nach eingehenden Beratungen im Bundestag, an denen ich beteiligt war, im Bundesgesetzblatt Teil I vom 22. August 1980 (S. 1429) verkündet.

In meinem 3. TB S. 12 f., habe ich mich ausführlich mit dem MRRG auseinandergesetzt. Viele meiner Vorschläge sind in die verabschiedete Fassung des Gesetzes übernommen worden. Insbesondere wurde meine Forderung nach einer klaren Aufgabenbeschreibung des Meldewesens und einer Festlegung des Datenkataloges verwirklicht.

§ 2 Abs. 3 MRRG erlaubt es den Bundesländern, in ihren Meldegesetzen zu bestimmen, daß für die Erfüllung von Aufgaben der Länder weitere als die in § 2 Abs. 1 und Abs. 2 MRRG festgelegten Daten gespeichert werden. Die im Regierungsentwurf zum MRRG hierzu noch vorgesehene Zweckbindung dieser zusätzlichen Daten an die Aufgaben der Meldebehörden, nämlich Identitätsfeststellung und Wohnungsnachweis, ist in der geltenden Fassung des Gesetzes leider nicht mehr vorhanden. Ich habe daher mehrfach der Hoffnung Ausdruck gegeben, daß die Landesgesetzgeber von dieser Ermächtigung in § 2 Abs. 3 MRRG nur zurückhaltend Gebrauch machen, und habe versucht, hierauf zusammen mit meinen Kollegen in den Ländern und in enger Zusammenarbeit mit dem Bundesminister des Innern hinzuwirken. Der Bayerische Landesbeauftragte und ich hatten Gelegenheit, über den Unterausschuß „EDV im Einwohnerwesen" des Arbeitskreises II der Innenministerkonferenz beratend den in diesem Unterausschuß erarbeiteten Formulierungsvorschlag für ein Landesmeldegesetz zu beeinflussen und den Datenschutz stärker zur Geltung zu bringen. Auch hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit einer Stellungnahme vom 2. April 1981 zu diesem Formulierungsvorschlag zu verhindern versucht, daß in den Landesmeldegesetzen das Volumen der Daten zu sehr erweitert wird und den Meldebehörden Aufgaben zugewiesen werden, die mit dem Inhalt des MRRG und den damit angestrebten Zielen nichts oder wenig zu tun haben.

Zum Zeitpunkt der Fertigung dieses Berichtes hatten alle Bundesländer Entwürfe für Landesmeldegesetze vorgelegt oder bereits verabschiedet und in Kraft gesetzt (so Bremen, Hamburg, Hessen, Nordrhein-Westfalen). Die inhaltliche Würdigung der Landesmeldegesetze ist Aufgabe meiner Kollegen in den Ländern. Nach dem derzeitigen Sachstand ist anzumerken, daß alle verabschiedeten Landesmeldegesetze und alle Gesetzentwürfe — außer dem schleswig-holsteinischen — die Verwendung von Ordnungsmerkmalen zur Führung der Melderegister erlauben, die insoweit die Funktion des ursprünglich geplanten Personenkennzeichens erfüllen sollen, jedoch nur örtlich oder regional begrenzte Gültigkeit haben. In den meisten Gesetzen ist auch vorgesehen, daß diese Ordnungsmerkmale innerhalb der öffentlichen Verwaltung und an die öffentlich-rechtlichen Religionsgesellschaften übermittelt werden dürfen. Ferner ist in einer Reihe von Landesgesetzen die Speicherung der Seriennummer des Passes oder des Personalausweises vorgesehen, was mit verschiedenen Aufgaben begründet wird: z. B. Feststellung der Identität des Einwohners oder Gefahrenabwehr und Strafverfolgung. In den Ausschußberatungen des 8. Deutschen Bundestages war nach eingehender Diskussion auch mit Vertretern der Länder die Speicherung der Seriennummer des Passes oder des Personalausweises für nicht erforderlich gehalten worden, um die Aufgaben der Meldebehörden sachgerecht zu erfüllen. Die beteiligten Vertreter der Sicherheitsbehörden

des Bundes hatten sich dieser Auffassung damals vorbehaltlos angeschlossen. Wenn die Seriennummer nunmehr über die Landesgesetze in den Datenkatalog des Melderegisters Eingang findet, so widerspricht dies eindeutig den Intentionen des Bundesgesetzgebers, zumal diese Entscheidung mit Argumenten begründet wird, die seinerzeit erörtert und als nicht stichhaltig verworfen worden sind.

Ein weiteres Datum, dessen Speicherung im Bundestag diskutiert und schließlich abgelehnt worden war, ist die Berufsangabe. Einige Länder halten jedoch das im MRRG vorgesehene Merkmal „erwerbstätig/nicht erwerbstätig" (§ 2 Abs. 1 Nr. 8 MRRG) nicht für ausreichend und erlauben deshalb im Landesgesetz die zusätzliche Speicherung der Berufsangabe. Auch hier wird mit Aufgaben der Länder begründet, was der Bundesgesetzgeber zuvor anders entschieden hat.

Die meisten der mit dem MRRG angestrebten bereichsspezifischen Datenschutzvorschriften sind indessen in die Landesgesetze bzw. deren Entwürfe übernommen worden. Diese Regelungen sind als abschließend angesehen und durch Landesrecht im wesentlichen nicht verändert worden. So bleibt festzustellen, daß jedenfalls insoweit die Rechtseinheitlichkeit in allen Ländern erreicht, ein notwendiges und im ganzen ausreichendes Maß an Datenschutz im Meldewesen gewährleistet werden kann und es damit gelungen ist, wesentliche Ziele des MRRG zu verwirklichen.

In § 20 Abs. 1 MRRG ist die Bundesregierung ermächtigt, durch Rechtsverordnung festzulegen, welche Daten für welche Zwecke *regelmäßig* an Behörden und andere öffentliche Stellen des Bundes übermittelt werden sollen. Eine regelmäßige Datenübermittlung wäre auch jede on-line-Verbindung zwischen Meldebehörden und Bundesbehörden.

Nach dem mir vorliegenden Entwurf einer Rechtsverordnung sind zur Zeit lediglich folgende regelmäßige Übermittlungen vorgesehen:

— Um zu vermeiden, daß Kindergeld weiterhin gezahlt wird, obwohl die Voraussetzungen dafür nicht mehr vorliegen, werden der Bundesanstalt für Arbeit einige wenige Daten von denjenigen Einwohnern übermittelt, zu denen minderjährige Kinder mit gleicher Anschrift gemeldet sind. Dies sind die ersten fünf Buchstaben des Familiennamens, der Tag der Geburt und die Gemeindekennzahl. Außerdem werden Tag der Geburt und gegebenenfalls Sterbetag des minderjährigen Kindes übermittelt.

  Durch einen automatisierten Abgleich kann die Bundesanstalt für Arbeit dann feststellen, ob ihre Zahlungen zu Recht erfolgen. Daß dazu auch in den Fällen Daten übermittelt werden, in denen kein Kindergeld gezahlt wird, kann hingenommen werden, weil der Abgleich in einer Weise erfolgt, die sicherstellt, daß dabei die Daten nicht zur Kenntnis genommen werden. Der Vorteil dieser Regelung liegt darin, daß die Meldebehörden nicht erfahren, an wen die Bundesanstalt für Arbeit Kindergeld zahlt. Für die Betroffenen entfällt die Vorlage der sogenannten Lebensbescheinigung für die Kinder.

— Um zu verhindern, daß über den Tod des Empfängers hinaus Renten (zu Unrecht) weitergezahlt werden, sollen bei Sterbefällen zukünftig regelmäßig Daten an den Rentendienst der Deutschen Bundespost übermittelt werden.

  Damit wird es möglich sein, die Überzahlungen in Höhe von mehr als 300 Mio. DM pro Jahr, von denen zur Zeit etwa 47 Mio. DM nicht rückrufbar sind, drastisch zu senken und auch den durch Überzahlungen verursachten Verwaltungsaufwand von etwa 7,5 Mio. DM zu verringern.

Der Entwurf dieser Rechtsverordnung wurde in enger und konstruktiver Zusammenarbeit mit dem Bundesminister des Innern von mir mitgestaltet. Zur Formulierung der entsprechenden Vorschriften wurden gemeinsame Besprechungen mit dem Bundesminister für Arbeit und Soziales und dem Bundesminister für das Post- und Fernmeldewesen geführt. Dabei konnte ich aufgrund des in meiner Dienststelle vorhandenen Querschnittswissens über die Funktion und die Informationsabhängigkeiten der öffentlichen Verwaltung insbesondere dazu beitragen, daß der Datenfluß zweckmäßig und wirtschaftlich geregelt wurde. Die gefundenen Regelungen werden zu einem transparenten und kontrollierbaren Verfahren führen, das den Anforderungen des Datenschutzes entspricht.

Die regelmäßigen Übermittlungen personenbezogener Daten an die Wehrersatzbehörden und gegebenenfalls an das Bundesamt für den Zivildienst konnten bisher noch nicht in dem Entwurf der Rechtsverordnung nach § 20 Abs. 1 MRRG berücksichtigt werden, weil vorher das Wehrpflichtgesetz und das Zivildienstgesetz in den Bestimmungen geändert werden sollten, die die Mitteilungspflichten der Meldebehörden regeln. In einer Besprechung mit dem Bundesminister für Jugend, Familie und Gesundheit und in einer Ressortbesprechung beim Bundesminister der Verteidigung habe ich meine Erwartungen an die gesetzlichen Neuregelungen und meine Anregungen vorgetragen. Sie wurden in die Stellungnahme der Bundesregierung übernommen. Auch hierbei wurde ich primär mit dem Ziel beteiligt, datenschutzrechtliche Bedenken von vornherein zu vermeiden, um die Durchsetzung der Lösung zu erleichtern. Im Laufe der Diskussion ergab sich daraus der konstruktive Vorschlag zu einem einfachen, datenschutzgerechten und wirksamen Verfahren. Das Artikelgesetz zur Änderung des Wehrrechts und des Zivildienstrechts ist vom Deutschen Bundestag im Dezember 1982 verabschiedet worden.

Gemäß § 20 Abs. 2 MRRG kann der Bundesminister des Innern durch Rechtsverordnung die sogenannte Rückmeldung zwischen den Meldebehörden gemäß § 17 MRRG regeln. Durch diese Verordnung soll festgelegt werden, welche Daten regelmäßig zwischen Meldebehörden *verschiedener Bundesländer* übermittelt werden, wenn ein Einwohner von einem Bundesland in ein anderes umgezogen ist. Die

Rückmeldung bei Umzügen innerhalb eines Bundeslandes kann nur durch Landesrecht geregelt werden; hier werden voraussichtlich mindestens die gleichen Daten übermittelt werden.

Auch dieser Entwurf einer Rechtsverordnung wurde zusammen mit dem Bundesminister des Innern an die Anforderungen des Datenschutzes angepaßt. Der Bundesminister des Innern geht davon aus, daß die Entwürfe Anfang 1983 verabschiedet werden können.

Ich würde es begrüßen, wenn es mir ermöglicht würde, stets so frühzeitig wie in diesen Fällen meinen Rat bei der Gestaltung von Rechtsvorschriften, die die Verarbeitung personenbezogener Daten regeln, einbringen zu können.

Die Verordnungen nach § 20 MRRG legen für die in den Verordnungen bestimmten regelmäßigen Datenübermittlungen den *„Datensatz für das Meldewesen“* zugrunde. Dieser Datensatz basiert auf dem Übermittlungsdatensatz, der entwickelt wurde, als die Einführung eines bundeseinheitlichen Personenkennzeichens und die Bildung von Landesadreßregistern erwartet wurde.

Der „Datensatz für das Meldewesen“ wurde zwischenzeitlich den Anforderungen des MRRG angepaßt. Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat 1981 eine gemeinsame Stellungnahme zu diesem Datensatz abgegeben. Die Arbeitsgruppe hat jedes Feld auf seine Rechtmäßigkeit überprüft und in Zweifelsfällen die Streichung bzw. die Klärung der Erforderlichkeit des Feldes gefordert. Aber auch Initiativen einzelner Landesbeauftragter haben mit dazu beigetragen, daß der jetzt von allen Innenministern und Innensenatoren gebilligte „Datensatz für das Meldewesen“ in Umfang und Inhalt reduziert und datenschutzgerechter geworden ist.

Bemerkenswert ist, daß dieser Datensatz von jedermann bezogen werden kann und für jedermann zugänglich beim Bundesarchiv niedergelegt wird. Damit ist es gelungen, einen Aufgabenbereich der öffentlichen Verwaltung in allen seinen Phasen transparent zu gestalten. Von vielen ist seinerzeit befürchtet worden, daß die Handlungsfreiheit der Meldebehörden unangemessen eingeschränkt würde, wenn das Melderecht „weiter so verrechtlicht werde“. Diese Sorge hat sich als unbegründet erwiesen. Denn die bisherige Entwicklung hat gezeigt, daß der Zwang, Datenbedarf präzise zu begründen und seine Verwendung darzulegen, durchaus nützlich sein kann. Mit der Neugestaltung des Melderechts wurde in der bereichsspezifischen Datenschutzgesetzgebung ein Weg beschritten, der m. E. beispielhaft für noch weitere Rechtsgebiete sein sollte.

2.1.2 Wahlrecht

Der Bundesminister des Innern hat mich vor kurzem wissen lassen, daß demnächst eine Novellierung der Bundeswahlordnung anstehe. Dabei sollen die früher erreichten Verbesserungen des Datenschutzes (vgl. 1. TB S. 40 und 2. TB S. 10ff.) unberührt bleiben. Hierzu zählen namentlich

— das Recht des Betroffenen, die Unkenntlichmachung des Geburtsdatums während der Auslegung des Wählerverzeichnisses zu verlangen (§ 21 Abs. 3 BWO);

— die Regelung, daß Auszüge oder Abschriften aus dem Wählerverzeichnis die Geburtstage der Wahlberechtigten nicht enthalten dürfen sowie nur für Zwecke der Wahl verwandt und Dritten nicht zugänglich gemacht werden dürfen (§ 21 Abs. 4 Satz 2 und 3 BWO).

— Regelungen, die die Wahlorgane zur Verschwiegenheit verpflichten (§ 5 Abs. 5, § 6 Abs. 3 BWO) und den Mitgliedern des Wahlvorstandes untersagen, Angaben zur Person des Wählers — soweit es nicht die Feststellung der Wahlberechtigung erfordert — so zu verlautbaren, daß sie von sonstigen im Wahlraum Anwesenden zur Kenntnis genommen werden können (§ 56 Abs. 4 BWO).

Mir sind keine Fälle bekannt, aus denen sich das Bedürfnis nach Änderung des geltenden Rechts ergeben könnte. Das Wahlverfahren scheint allen datenschutzrechtlichen Anforderungen zu genügen.

2.1.3 Ausländerzentralregister

Das Bundesverwaltungsamt führt in Gestalt des Ausländerzentralregisters eine umfassende Datei. Sie enthält mehrere Mio. Datensätze mit zahlreichen Angaben über die von den Ausländerbehörden erfaßten Ausländer, die nicht nur vorübergehend in der Bundesrepublik Deutschland gemeldet sind.

Im Jahre 1980 hatte ich eine Prüfung des beim Bundesverwaltungsamt geführten Ausländerzentralregisters vorgenommen und darüber in meinem Dritten Tätigkeitsbericht (S. 16) berichtet. Ich hatte insbesondere Zweifel daran geäußert, ob die vom Ausländerzentralregister gespeicherten Daten von der Ermächtigung des § 6 des Gesetzes über die Errichtung des Bundesverwaltungsamtes gedeckt werden. Danach dient das Ausländerzentralregister lediglich „der Erfassung von im Bundesgebiet wohnhaften Ausländern“.

Den Bundesminister des Innern habe ich Ende 1980 über meine Bedenken unterrichtet und ihn um Stellungnahme gebeten. Im Sommer 1981 wurde ich auf Anfrage darüber informiert, daß mein Bericht sowie die unabhängig davon geplante Neukonzeption des Ausländerzentralregisters dem Bundesminister des Innern Veranlassung gegeben haben, die Datenverarbeitung durch das Ausländerzentralregister einer grundsätzlichen Prüfung zu unterziehen. Erst auf erneute mehrfache Anfragen hat mir der Bundesminister im Herbst 1982 mitgeteilt, die Prüfungsergebnisse hätten bislang noch nicht abschließend bewertet werden können. Eine erste rechtliche Würdigung führe seiner Auffassung nach dazu, daß die Datenverarbeitung durch das Ausländerzentralregister auf der Grundlage des geltenden Rechts grundsätzlich als abgesichert angesehen werden könne. Damit sei aber noch nicht die Frage beantwortet, ob

es aus rechtspolitischen Gesichtspunkten zweckmäßig erscheine, bei passender Gelegenheit eine Verbesserung der gesetzlichen Formulierungen anzustreben, um hinsichtlich der Aufgabenstellung und Arbeitsweise des Ausländerzentralregisters noch mehr Transparenz zu erreichen. Es sei allerdings verfrüht, so führt der Bundesminister des Innern weiter aus, schon jetzt in gesetzgeberische Überlegungen einzutreten. Er halte es vielmehr zunächst für angezeigt, Fragen zur Aufgabenstellung des Ausländerzentralregisters, zur Ausgestaltung der Datenverarbeitung sowie zur Kommunikation mit den Bedarfsträgern im einzelnen zu klären.

Ich habe mich bemüht, den im Sommer 1982 fertiggestellten Prüfbericht des Bundesministers des Innern, in dem auch meine Bemerkungen über das Ausländerzentralregister aus dem Jahre 1980 behandelt sind, zu erhalten. Aufgrund mehrfacher Bitten ist mir der Bericht Mitte Dezember 1982 übersandt worden. Bislang konnte ich nur eine erste Durchsicht vornehmen.

Den Fortgang der Angelegenheit werde ich aufmerksam beobachten und halte es weiterhin für notwendig, an den Bemühungen um eine Neukonzeption des Ausländerzentralregisters beratend beteiligt zu sein.

2.1.4 Bundesamt für den Zivildienst

Schon 1979 hat sich ein Zivildienstleistender beschwerdeführend an mich gewandt: Er habe von dem Beauftragten für Kriegsdienstverweigerer und Zivildienstleistende seiner Landeskirche unaufgefordert eine kirchliche Zeitschrift nebst Begleitbrief erhalten. Der Beschwerdeführer stellte die Notwendigkeit der Weitergabe der diesem Verfahren zugrundeliegenden Daten an die Kirchen in Frage. Auch fürchtete der Beschwerdeführer, daß seine Daten in einer derart großen Organisation wie der Kirche nicht hinreichend geschützt seien.

Inzwischen ist die Erhebung und Weitergabe von Daten über die Religionszugehörigkeit von Wehrpflichtigen und Zivildienstleistenden mit Vertretern der Kirchen, dem Bundesamt für den Zivildienst (BAZ), dem Bundesbeauftragten für den Zivildienst, dem Bundesminister für Arbeit und Sozialordnung, dem Bundesminister für Jugend, Familie und Gesundheit (der seit Anfang 1982 für den Zivildienst zuständig ist) sowie mit dem Bundesminister der Verteidigung erörtert worden. Diese Erörterung ist noch immer nicht abgeschlossen; doch ist ein Schritt in die richtige Richtung gemacht worden: Das BAZ hat im sogenannten „Anhörungsbogen" die Beantwortung der Frage nach der Religionszugehörigkeit unter Hinweis auf § 9 Abs. 2 BDSG freigestellt. Im Einklang hiermit hat das BAZ in „Hinweisen für anerkannte Kriegsdienstverweigerer" den Zivildienstleistenden die Entscheidung eingeräumt, diejenigen Daten, die dem BAZ von der Bundeswehr übermittelt werden, im Datenbestand der BAZ löschen zu lassen und damit eine Übermittlung an die katholische bzw. evangelische Kirche auszuschließen. Unbeschadet der rechtlichen und statusmäßigen Unterschiede zwischen Militärseelsorge einerseits und Seelsorge für Zivildienstleistende andererseits habe ich dem Bundesminister der Verteidigung nahegelegt, die vom BAZ getroffene Lösung, die Antwort auf die Frage nach der Religionszugehörigkeit dem Betroffenen freizustellen, für die Bundeswehr zu übernehmen. Schon die praktische Frage, ob Angaben über die Religionszugehörigkeit, die von dem Betroffenen nicht freiwillig gemacht worden sind, für die Seelsorge überhaupt dienlich, geschweige denn erforderlich sind, ist m. E. zu verneinen. Von einem Wehrdienstpflichtigen, der nicht von sich aus bereit ist, seine Religionszugehörigkeit zu offenbaren, dem dies vielmehr als Pflicht auferlegt wird, kann m. E. eine Bereitschaft zu einer gezielten Ansprache durch die Seelsorge nicht angenommen werden.

Die rechtliche Betrachtung hat von der Frage auszugehen, ob die Religionszugehörigkeit von dem Wehrpflichtigen überhaupt erfragt werden darf. Erst hieran schließt sich die weitere Frage an, ob eine Pflicht zur Angabe seiner Konfessionszugehörigkeit besteht. Wiederum davon zu unterscheiden ist, ob es zulässig ist, die Religionsangabe an das BAZ und von diesem an die Religionsgesellschaften — soweit es sich um Zivildienstleistende handelt — bzw. an Stellen der Militärseelsorge — soweit es sich um Wehrdienstleistende handelt — zu übermitteln. Nach Artikel 136 Abs. 3 Satz 2 Weimarer Reichsverfassung (WRV) i. V. m. Artikel 140 GG besteht das Fragerecht insoweit, als davon — genauer von der Antwort — „Rechte und Pflichten abhängen". Ich habe mich davon überzeugt, daß die Verwirklichung sowohl des Individualrechts des Soldaten nach § 36 Soldatengesetz auf Seelsorge als auch das den Kirchen eingeräumte Recht auf staatliche Organisation der Militärseelsorge die Befragung aller Soldaten nach ihrer Konfessionszugehörigkeit notwendig macht. Die Konfessionsangabe ist nötig für die Feststellung der Planstellenzahl und den Zuschnitt der Seelsorgebezirke.

Eine generelle Pflicht des einzelnen Soldaten bzw. Wehrpflichtigen zur Angabe seiner Konfessionszugehörigkeit besteht jedoch nach staatlichem Recht nicht. Selbstverständlich kann der Militärgeistliche die Soldaten, die seine Seelsorge erbitten oder Amtshandlungen beantragen, nach ihrer Konfessionszugehörigkeit fragen, und aus dienstrechtlichen Gründen können auch die militärischen Vorgesetzten einen Soldaten, der von seinem Recht auf Seelsorge Gebrauch machen will, fragen, ob er überhaupt der betreffenden Konfession angehört. Ich bin jedoch nicht davon überzeugt, daß der Soldat nach staatlichem Recht auch sonst zur Antwort verpflichtet ist; er ist es m. E. insbesondere dann nicht, wenn er von dem kirchlichen Angebot gar keinen Gebrauch machen will.

Ich halte es also nicht nur für ratsam, sondern für rechtlich geboten, daß die Antwort dem Wehrpflichtigen bzw. Soldaten freigestellt bleibt. Er ist gemäß § 9 Abs. 2 BDSG auf die Freiwilligkeit der Angaben hinzuweisen.

Die weitere Frage, welche Auswertung der erhobenen Angaben zulässig ist, läßt sich nicht mehr aus

Artikel 136 Abs. 3 WRV beantworten, sondern aus dem Bundesdatenschutzgesetz. Dabei dürfte wie folgt zu unterscheiden sein:

— Für die Planung und Organisation der Militärseelsorge genügt nach meiner Auffassung die Übermittlung *statistischer* Daten.

— Klärungsbedürftig scheint mir hingegen noch, inwieweit die Angabe über die Konfessionszugehörigkeit des einzelnen Soldaten für die Ausübung der Militärseelsorge erforderlich ist. Meines Erachtens könnte es genügen, daß der zuständige Militärseelsorger in den Kasernen auf Gottesdienste, Sprechstunden usw. hinweist.

Für Zivildienstleistende stellt sich die Rechtslage anders dar als bei den Soldaten. Während Soldaten an ihrem Stationierungsort keiner Meldepflicht unterliegen, wenn sie in einer Gemeinschaftsunterkunft wohnen, so daß die Kirchen die Daten ihrer Mitglieder nur von der Bundeswehr erhalten können, müssen sich die Zivildienstleistenden an ihrem Wohnort bei der Meldebehörde anmelden und die Kirche erhält von der Meldebehörde die Anschrift. Außerdem fehlen für den Zivildienst besondere vertragliche und gesetzliche Regelungen, wie sie für die Militärseelsorge bestehen. Nach Datenschutzrecht ist daher zu fragen, ob die Übermittlung von Daten über die Religionszugehörigkeit der Zivildienstleistenden von der Bundeswehr an das Bundesamt für den Zivildienst und von dort an die kirchlichen Stellen (die hier — anders als bei der Militärseelsorge — nicht in die staatliche Organisation eingegliedert sind) erforderlich ist.

Ich erkenne an, daß die Kenntnis der Konfessionsverteilung erforderlich sein kann, um besondere seelsorgerische Einrichtungen für den Zivildienst vorzuhalten. Damit wäre aber wiederum nur die statistische Auswertung der insofern zulässigen Fragen und der hierauf erhaltenen Antworten gerechtfertigt.

Entscheidend ist aus meiner Sicht, daß die Freiwilligkeit der Angaben gesichert ist. Nach § 9 Abs. 2 BDSG ist ein entsprechender Hinweis zu geben. Darüber hinaus wäre zu erwägen, ob nicht angesichts dieser Freiwilligkeit beim ersten Schritt, der Datenerhebung, auch für den zweiten Schritt, die Übermittlung, soweit sie für erforderlich gehalten wird, die Einwilligung als Rechtfertigungsgrund gewählt werden sollte. Der Aufwand hierfür wäre gering und dem Willen des einzelnen wäre stärker Rechnung getragen.

2.1.5 Anerkennungsverfahren für Kriegsdienstverweigerer

In meinem letzten Tätigkeitsbericht (S. 7) habe ich im Bereich des Anerkennungsverfahrens für Kriegsdienstverweigerer eine besondere Behandlung der in diesem Verfahren beim Bundesamt für den Zivildienst entstehenden Akten gefordert. Der Bundesminister für Jugend, Familie und Gesundheit hat meiner Anregung insofern entsprochen, als er angeordnet hat, daß die Verfahrensprotokolle gesondert unter Verschluß zu nehmen sind. Da aber nicht nur diese Protokolle, sondern auch der Antrag auf Anerkennung, den der Betroffene eingehend zu begründen hat, sowie die beizufügenden Zeugenaussagen Daten von sehr hohem Sensibilitätsgrad enthalten, habe ich vorgeschlagen, auch diese Unterlagen in die vorgesehene Regelung einzubeziehen. Ich begrüße es, daß sich der Bundesminister für Jugend, Familie und Gesundheit diesen Überlegungen ebenfalls angeschlossen und das Bundesamt für den Zivildienst angewiesen hat, lediglich den Anerkennungsbescheid (ohne Begründung) zu den Personalakten zu nehmen und die übrigen Unterlagen getrennt und unter besonderem Verschluß aufzubewahren.

2.1.6 Bundesnotaufnahmeverfahren

Im Rahmen einer Prüfung haben meine Mitarbeiter die Dienststellen des Notaufnahmeverfahrens in Berlin-Marienfelde und Gießen besucht. Die Erforderlichkeit der Angaben im Antrag auf Notaufnahme, die Zentrale Namenskartei sowie die Heimatortskartei bildeten dabei die Schwerpunkte. Insgesamt habe ich den Eindruck gewonnen, daß sich die Mitarbeiter dieser Dienststellen ihrer Verantwortung bewußt sind und mit den ihnen anvertrauten besonders sensiblen und schutzbedürftigen Daten sorgfältig umgehen. Nichtsdestoweniger habe ich in den vorgenannten Prüfungsschwerpunkten Verbesserungsvorschläge und Anregungen gegenüber dem Bundesminister des Innern gemacht. Sie werden derzeit dort geprüft.

2.1.7 Heimkehrerstiftung

Nach dem Kriegsgefangenenentschädigungsgesetz gewährt die Heimkehrerstiftung — Stiftung für ehemalige Kriegsgefangene — Darlehen, einmalige Unterstützungen zur Linderung einer Notlage und Renten. Dazu muß sie eine Reihe von Angaben über das Schicksal der Betroffenen erheben und speichern. Meine Mitarbeiter haben die Art und Weise, in der diese sensiblen Daten verarbeitet werden, eingehend geprüft. Ich habe angeregt, die Ermächtigung, um die der Antragsteller gebeten wird und mit deren Hilfe die zuständigen Behörden gegebenenfalls um Auskunft über persönliche und wirtschaftliche Verhältnisse des Betroffenen ersucht werden, transparenter zu gestalten. Dem Betroffenen sollte verdeutlicht werden, welche Behörden gegebenenfalls um Auskunft ersucht werden können. Die Prüfung hat außerdem Schwachstellen im Bereich der Datensicherung erkennen lassen. Die Heimkehrerstiftung hat sich gegenüber meinen Anregungen aufgeschlossen gezeigt und ist bemüht, Abhilfe zu schaffen.

2.1.8 Stiftung für ehemalige politische Häftlinge

Jeder gemäß § 10 des Häftlingshilfegesetzes anerkannte politische Häftling kann sich an die Stiftung für ehemalige politische Häftlinge mit der Bitte um eine einmalige finanzielle Unterstützung wenden. Das Verfahren ist in einem besonderen Merkblatt geregelt, welches die Angabe von personenbezoge-

nen Daten in einem entsprechenden Antragsformular vorsieht. Diese Daten sind besonders schutzwürdig. Meine Mitarbeiter haben sich im Rahmen einer Prüfung davon überzeugen können, daß die Stiftung bei der Behandlung der Daten die gebotene Sorgfalt anwendet und die Vorschriften des Bundesdatenschutzgesetzes einhält.

2.2 Rechtswesen

2.2.1 Bundeszentralregister

Das Bundeszentralregister war seit Beginn meiner Tätigkeit Gegenstand besonderer Aufmerksamkeit. Ich habe wiederholt Prüfungen durchgeführt und spürbare Verbesserungen der Datensicherung feststellen können.

Schon bei früherer Gelegenheit habe ich das Bundeszentralregistergesetz als Beispiel eines gelungenen bereichsspezifischen Datenschutzgesetzes bezeichnet. In meiner Stellungnahme zu dem im Frühjahr 1981 vorgelegten Referentenentwurf eines Zweiten Gesetzes zur Änderung des Bundeszentralregistergesetzes, der inzwischen als Regierungsvorlage (Drucksache 9/2068) beim Deutschen Bundestag eingebracht worden ist, habe ich jedoch zum Ausdruck gebracht, daß der Gesetzgeber die Gelegenheit einer Novellierung nutzen sollte, um zu prüfen, ob die geltenden Regelungen dem gegenwärtigen Stand der Datenschutzdiskussion in vollem Umfange entsprechen. Meine dem Bundesminister der Justiz zugeleiteten Vorschläge habe ich daher nicht auf den Entwurf beschränkt, sondern die sonstigen Vorschriften des Bundeszentralregistergesetzes mit einbezogen.

Um die Zielrichtung meiner Vorschläge zu verdeutlichen, möchte ich zwei Beispiele, die ich schon in meinem Vierten Tätigkeitsbereicht angegeben habe, nochmals nennen:

— Nach § 10 BZRG sind gerichtliche Entscheidungen einzutragen, durch die jemand entmündigt wird. Im Gegensatz zur Tilgung von Vorstrafen ist eine Löschung der Eintragung nicht vorgesehen. Wird die Entmündigung wieder aufgehoben, ist vielmehr auch diese Entscheidung einzutragen. Der Gesetzgeber sollte erwägen, die Eintragung entweder von Amts wegen zu löschen oder doch zumindest die Möglichkeit einer Löschung auf Antrag vorzusehen (vgl. 4. TB S. 42).

— Nach § 12 BZRG sind u. a. gerichtliche Entscheidungen und Verfügungen einer Strafverfolgungsbehörde einzutragen, durch die eine Strafverfolgung wegen Schuldunfähigkeit abgeschlossen wird. Diese Eintragung wird — ebenso wie die zuvor erwähnte — nicht getilgt, sondern bleibt bis zum Tode, spätestens bis zum 90. Lebensjahr im Register erhalten. Auch dies sollte geändert werden.

Ein weiteres Beispiel möchte ich hinzufügen:

— Nach § 39 Abs. 1 Nr. 2 BZRG ist den obersten Bundes- und Landesbehörden für jeden beliebigen Zweck die unbeschränkte Auskunft zu erteilen. Dieses Recht wird gelegentlich dazu benutzt, um für nachgeordnete Behörden Auskünfte einzuholen, die diese nicht selbst bekommen würden. Oberste Bundes- und Landesbehörden erfüllen in der Regel keine Aufgaben, die Entscheidungen über Einzelpersonen erforderlich machen. Sie unterscheiden sich damit von den sonstigen in § 39 Abs. 1 aufgeführten Stellen. Eine unbeschränkte Auskunft erscheint mir nur in denjenigen Fällen der Einstellung von Personal gerechtfertigt, in denen diese mit einer Sicherheitsüberprüfung verknüpft ist. Ich würde es begrüßen, wenn die obersten Bundes- und Landesbehörden sich auf die Informationen beschränkten, die sie zur Erfüllung ihrer Aufgaben unbedingt benötigen.

Meine Vorschläge sind in dem Entwurf eines Zweiten Gesetzes zur Änderung des Bundeszentralregistergesetzes nicht berücksichtigt worden. Der Bundesminister der Justiz hat mir hierzu mitgeteilt, der Entwurf wolle das BZRG in erster Linie an die neuere Rechtsentwicklung, insbesondere an das Gesetz zur Neuordnung des Betäubungsmittelrechts, anpassen. Von Weiterungen, die zu einer Verzögerung des Gesetzgebungsverfahrens führen könnten, sei daher bewußt abgesehen worden. Diese Reaktion des Bundesministers der Justiz ist für mich nicht befriedigend, zumal der Bundesminister gleichzeitig zum Ausdruck gebracht hat, daß er einem wesentlichen Teil meiner Überlegungen „nicht ohne Sympathie gegenüberstehe". Ich habe meine Empfehlungen nunmehr dem für die Beratung des Gesetzes federführenden Rechtsausschuß des Deutschen Bundestages zugeleitet.

Die schon oben angesprochene Vorschrift des § 39 Abs. 1 Nr. 2 BZRG, die den obersten Bundes- und Landesbehörden, nicht aber nachgeordneten Behörden, ein Recht unbeschränkter Auskunft aus dem Register gewährt, spielt auch bei meinen Kontrollen der Datenübermittlung aus dem Register eine besondere Rolle. Dabei kommt es darauf an sicherzustellen, daß die nach geltendem Recht bestehende Limitierung des Auskunftsrechts nicht dadurch umgangen wird, daß die obersten Bundes- oder Landesbehörden über den durch § 41 BZRG gezogenen Rahmen hinaus Auskünfte für nachgeordnete oder ihrer Aufsicht unterstehende Behörden einholen und an diese weiterreichen. Zu diesem Zwecke habe ich mir vom Bundeszentralregister stichprobenmäßig Aufstellungen über die Ersuchen oberster Bundes- und Landesbehörden vorlegen lassen. Hierin gelegentlich festgestellte Zweckangaben wie „Feststellung der Eignung als Kleinsiedler", „Zuerkennung der fachlichen Eignung zur Ausbildung im Beruf Tankwart" oder „Bürgschaftseinzelsache" lassen darauf schließen, daß die Grenzen, die der unbeschränkten Auskunft gesetzt sind, nicht immer eingehalten werden — die angegebenen Verwaltungsvorgänge sind keine ministeriellen Aufgaben.

Gestützt auf § 19 Abs. 3 BDSG, wonach ich im Rahmen meiner Kontrollaufgaben Auskünfte sowie Einsicht in alle Unterlagen und Akten verlangen kann, die „im Zusammenhang mit der Verarbeitung

personenbezogener Daten stehen", vertrete ich die Auffassung, daß mir die Befugnis zusteht, die Zulässigkeit der Datenübermittlungen nach dem Bundeszentralregistergesetz auch durch Einsichtnahme in die einschlägigen Akten der Datenempfänger, so z. B. des Bundesjustizministeriums, zu kontrollieren. In Abstimmung mit dem Bundesminister des Innern hat dies der Bundesminister der Justiz insoweit eingeräumt, als die Datenübermittlung an die obersten Bundesbehörden und die für ihre Zulässigkeit vorausgesetzte Schlüssigkeit der Zweckangabe nach § 39 Abs. 4 BZRG Gegenstand der Kontrolle sind. Einer Prüfung der Zulässigkeit der Weitergabe an nachgeordnete Behörden gemäß § 41 BZRG haben die genannten Bundesressorts jedoch mit der Begründung widersprochen, daß es sich insoweit um eine Übermittlung aus Akten, namentlich aus Sicherheitsakten, nicht aus Dateien, handele. Gegen diese Auffassung spricht nicht nur der tatsächliche Zusammenhang; auch der Wortlaut des § 19 Abs. 1 Satz 1 BDSG, der mir ohne einen Dateibezug aufgibt, die Einhaltung „anderer Vorschriften über den Datenschutz", so des Bundeszentralregistergesetzes, zu kontrollieren, veranlaßt mich, der Auffassung der genannten Bundesressorts entgegenzutreten.

Der Generalbundesanwalt, Dienststelle Bundeszentralregister, hat jetzt den Entwurf von Richtlinien zur Automatisierung des Auskunftsverfahrens vorgelegt. In der ersten, für 1983 vorgesehenen Phase sollen die Anfragen zunächst auf Magnetbändern, baldmöglichst auch mit Hilfe des Teletex-Verfahrens dem BZR zugeleitet werden. Die Auskünfte selbst werden zunächst grundsätzlich schriftlich erteilt. Auch schon für diese Projektphase wird sorgfältig zu prüfen sein, welche technisch-organisatorischen Maßnahmen angesichts der hohen Sensibilität der übermittelten Daten ausreichende Sicherheit versprechen. Insbesondere wird zu prüfen sein, wie das Problem des „Leitvermerkes" für die Zusendung der Auskünfte zu lösen ist, d. h. wie sichergestellt werden kann, daß die Auskunft nur dem rechtmäßigen Empfänger zugeleitet wird. In einer zweiten Projektphase sollen auch die Auskünfte automatisiert, d. h. durch Datenträgeraustausch bzw. direkten Datenverkehr erteilt werden. Besonders wegen der geographischen Lage von Berlin-West werden hier besonders hohe Anforderungen an Datensicherungsmaßnahmen zu stellen sein. So halte ich eine Verschlüsselung der Auskünfte beim Datenverkehr zwischen Berlin-West und dem Bundesgebiet für unverzichtbar.

2.2.2 Mitteilungen in Strafsachen

Die Anordnung über Mitteilungen in Strafsachen (MiStra) ist eine interne Verwaltungsvorschrift, die vom Bundesminister der Justiz im Einvernehmen mit den Landesministern der Justiz erlassen worden ist. Sie regelt im einzelnen, unter welchen Voraussetzungen und in welchem Umfang Justizbehörden andere öffentliche Stellen über den Stand und die Ergebnisse von Strafverfahren zu unterrichten haben. Sie war wiederholt Gegenstand von Beratungen der Datenschutzbeauftragten des Bundes und der Länder. Vor dem Hintergrund der von ihnen im Jahre 1980 erhobenen Forderung, dem Datenschutz auch in diesem Bereich den ihm gebührenden Stellenwert beizumessen, sowie meines Dritten Tätigkeitsberichtes (S. 19), in dem ich diese Problematik erneut aufgegriffen habe, hat der Rechtsausschuß des Deutschen Bundestages im Jahre 1981 die Bundesregierung um Prüfung und um anschließenden Bericht gebeten, inwieweit die Bestimmungen der MiStra erforderlich sind, inwieweit sie in Gesetzesform gebracht werden sollten und in welcher Form die Betroffenen über solche Mitteilungen benachrichtigt werden könnten. Der Bundesminister der Justiz hat daraufhin erfreulicherweise mitgeteilt, daß ein mit der MiStra befaßter Unterausschuß der Justizministerkonferenz mit großer Mehrheit die Auffassung vertreten hat, es solle eine bundesgesetzliche Rechtsgrundlage (Ermächtigung des Bundesministers der Justiz zum Erlaß einer Rechtsverordnung mit Zustimmung des Bundesrates) angestrebt werden. Darüber hinaus anerkennen die Justizminister, daß es angebracht ist, den Umfang der Mitteilungspflichten mit dem Ziel einer Reduzierung zu überprüfen. Im Einklang mit meinen Vorschlägen solle daher geklärt werden, inwieweit es aus heutiger Sicht vertretbar erscheint, die jeweils widerstreitenden Interessen der Allgemeinheit und des Betroffenen (unabhängig vom konkreten Einzelfall) anders als bisher zu bewerten, so daß bestimmte Mitteilungspflichten entfallen oder inhaltlich reduziert werden können.

Der Bundesminister der Justiz hat mich inzwischen davon unterrichtet, daß sich die Arbeiten an der MiStra wegen der Berührungspunkte mit zahlreichen Rechtsgebieten und Belangen vieler Bundes- und Landesressorts wesentlich schwieriger und umfangreicher als erwartet gestalten. Gleichwohl seien Vorschläge zur Überarbeitung der MiStra von der hierfür eingesetzen Arbeitsgruppe entwickelt und den übrigen Justizverwaltungen übermittelt worden. Die Phase der Prüfung der übersandten Vorschläge sei noch nicht abgeschlossen.

Unabhängig von Einzelheiten einer bundesgesetzlichen Rechtsgrundlage für die MiStra hat der Bundesminister der Justiz zur Vorbereitung einer solchen Regelung bei den Landesjustizverwaltungen auch die Frage zur Diskussion gestellt, inwieweit außerhalb der MiStra in Verwaltungsvorschriften geregelte Mitteilungspflichten in Strafsachen mit einbezogen werden sollten.

Ich begrüße das sich abzeichnende Zwischenergebnis der Beratungen und werde in Abstimmung mit den Datenschutzbeauftragten der Länder die weitere Erörterung aufmerksam verfolgen.

2.2.3 Richtlinien für das Strafverfahren und das Bußgeldverfahren

Seit Jahren trete ich für eine Überarbeitung der Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977 (RiStBV) ein mit dem Ziel, auch hier mehr Datenschutz zu verwirklichen. Fortschritte bei diesen Bemühungen zeichnen

sich bislang leider erst in Ansätzen ab. Ich beschäftige mich mit diesen Richtlinien, die sich als Verfahrensanleitungen in erster Linie an den Staatsanwalt wenden, aber auch — wie die „Einführung" der Richtlinien sagt — „für den Richter von Bedeutung sein können", aus zwei Anlässen:

— Private Vereinigungen, die sich der Bekämpfung der Wirtschaftskriminalität widmen, gaben einen „Warndienst" heraus, in dem regelmäßig Strafurteile unter voller Angabe der Personalien Verurteilter mitgeteilt wurden, und zwar in einer Form, die es den Beziehern ermöglichte, sich auf verhältnismäßig einfache Weise eine alphabetisch geordnete Kartei anzulegen. Inzwischen ist — wie mir der Bundesminister der Justiz bestätigt hat — die Herausgabe des „Warndienstes" eingestellt worden. Meine dem Minister bereits 1979 erläuterten Bedenken (vgl. auch 2. TB S. 17) gegen die Übermittlung vollständiger Urteilsabschriften an die in Nr. 236 der Richtlinien genannten Stellen, die sich mit der Bekämpfung der Wirtschaftskriminalität befassen, sind hiermit aber nicht ausgeräumt. Die Übermittlung steht zu Zielen des Bundeszentralregistergesetzes in Widerspruch, durch Tilgung von Straftaten nach Fristablauf dem Verurteilten die Resozialisierung zu ermöglichen. Ich verkenne nicht die wichtige Funktion, die die genannten Einrichtungen bei der Abwehr der Wirtschaftskriminalität zu erfüllen haben. Diese Funktion wird jedoch zu einem wesentlichen Teil bereits dadurch erfüllt, daß z. B. die Arbeitsweise von Straftätern bekanntgemacht wird. Angaben über bestimmte Personen sind hierzu nicht erforderlich. Ich habe daher den Bundesminister der Justiz 1982 erneut um eine Stellungnahme zu meinem seinerzeit gemachten Vorschlag gebeten, zu übersendende Urteile zumindest ausreichend zu anonymisieren.

— Ein weiterer Anlaß, mich mit den Richtlinien zu befassen, waren Schwierigkeiten, auf die ein holländischer Bürger bei dem Bemühen stieß, Akten über seine 1943 wegen eines Bagatelldiebstahls erfolgte Verurteilung zu einer hohen Zuchthausstrafe einzusehen. Ich habe dem Bundesminister der Justiz bereits 1979 mitgeteilt, daß ich die gegenwärtige Fassung der Nr. 185 der Richtlinien, die dem Betroffenen eine Akteneinsicht grundsätzlich versagt und ihm auferlegt, hierzu einen Rechtsanwalt zu bevollmächtigen, für unbefriedigend halte. Für einen Angeklagten ist es oft sehr wichtig zu wissen, was über ihn in den Akten steht. Mir ist kein Grund ersichtlich, warum ein Angeklagter, der keinen Anwalt hat, insoweit schlechter gestellt sein soll. Die Gefahr einer Veränderung des Akteninhalts ließe sich dadurch vermeiden, daß dem Betroffenen die Akten in den Diensträumen der Staatsanwaltschaft oder des Gerichtes im Beisein eines Bediensteten vorgelegt werden. Ich habe dem Bundesminister der Justiz hierzu Formulierungsvorschläge zugehen lassen. Der Minister hat mir inzwischen mitgeteilt, daß Fragen des Akteneinsichtsrechts, namentlich des Beschuldigten bzw. Angeklagten, Gegenstand von Beratungen des zuständigen Unterausschusses der Justizministerkonferenz sind.

Meine Empfehlungen zu den Richtlinien haben sich auf die beiden genannten Problemkreise nicht beschränkt; auch zu anderen Punkten habe ich dem Bundesminister der Justiz Vorschläge unterbreitet: Zum Problem der Aufklärung der persönlichen und wirtschaftlichen Verhältnisse des Beschuldigten (Nr. 13 f. RiStBV) habe ich erfahren, daß in Einzelfällen — namentlich von freiberuflich Tätigen — Art und Inhalt der öffentlichen Vernehmung des Angeklagten zu seinen bzw. seines Ehegatten Einkommens- und Vermögensverhältnissen von ihm als eine stärkere Beeinträchtigung empfunden wird als die Strafe selbst, weil sie befürchten, daß ein Bekanntwerden ihrer geschäftlichen und wirtschaftlichen Verhältnisse zu Nachteilen und Einbußen führen kann.

Selbstverständlich darf der Grundsatz der Öffentlichkeit der Verhandlung nicht aufgegeben werden. Ich bin mir bewußt, daß datenschutzrechtliche Vorschriften nicht Platz greifen, wo es um den Umfang mündlicher Verhandlung vor Gericht geht. Ich habe gegenüber dem Bundesminister der Justiz gleichwohl angeregt, in die auf dem 54. Deutschen Juristentag begonnene Erörterung, ob die Vorschriften über die Öffentlichkeit des Strafverfahrens neu zu gestalten sind, um die Rechtstellung des Beschuldigten (und anderer Prozeßbeteiligter) zu verbessern, auch den hier aufgezeigten Aspekt einzubeziehen. Ich gebe zu erwägen, in geeigneten Fällen dem Beschuldigten (bzw. seinem Verteidiger) die schriftliche Darstellung der Einkommens- und Vermögensverhältnisse anheimzugeben und verstärkt von der Möglichkeit des § 249 Abs. 2 der Strafprozeßordnung Gebrauch zu machen, aufgrund eines Verzichtes der Verfahrensbeteiligten von der Verlesung eines solchen Schriftstückes abzusehen. Nummer 4 der Richtlinien könnte durch einen Hinweis auf diese Verfahrensmöglichkeit ergänzt werden.

In der Frage der Unterrichtung des Beschuldigten von Einstellungsverfügungen wegen Zurechnungsunfähigkeit (Nr. 88 RiStBV) sind insofern Fortschritte zu verzeichnen, als einige Landesjustizverwaltungen die Staatsanwaltschaften angewiesen haben, zu prüfen, ob der Betroffene auf die Eintragung im Bundeszentralregister und auf sein Antragsrecht nach § 23 Abs. 1 Satz 1 Bundeszentralregistergesetz hinzuweisen ist. Ich halte es für geboten, durch Neufassung der Nr. 88 RiStBV zu einer klärenden und einheitlichen Lösung zu gelangen.

2.2.4 Mitteilungen in Zivilsachen

Die Anordnung über Mitteilungen in Zivilsachen (MiZi) vom 1. Oktober 1967 war bereits Gegenstand meines Vierten Tätigkeitsberichtes (vgl. dort S. 43). Sie bezieht sich auf so vielfältige und so unterschiedliche Sachverhalte, daß ich selbst nicht erwarten konnte, mit der von mir vorgeschlagenen Überarbeitung bereits nach kurzer Frist am Ziel zu sein.

Die Mitteilungspflichten der MiZi haben fast ausnahmslos personenbezogene Daten zum Gegen-

stand: Finanzbehörden, Sozialbehörden, Staatsanwaltschaften, Standesämter und andere Registerbehörden sollen auf diesem Wege Informationen über gerichtliche Entscheidungen erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen. Bei der Mehrzahl der Mitteilungspflichten ist die Notwendigkeit offenkundig, vielfach ist die Mitteilung auch durch Rechtsvorschriften abgedeckt. Manche Fallgruppen aber müssen heute hinsichtlich ihrer rechtlichen Begründung und praktischen Notwendigkeit überprüft werden.

Von den Beispielen, die ich bereits in meinem vorigen Tätigkeitsbericht genannt habe, möchte ich zwei wiederholen:

— Die Staatsanwaltschaften sind zu unterrichten, wenn Verfahren zur Entmündigung wegen Geisteskrankheit oder Geistesschwäche eingeleitet werden. Schutzwürdige Belange des Betroffenen können erheblich beeinträchtigt werden, wenn das Verfahren nicht zur Entmündigung führt, die Unterlagen aber bei der Staatsanwaltschaft bleiben, ohne daß der Betroffene davon weiß.

— Bei Räumungsklagen wegen Zahlungsverzugs des Mieters ist der örtliche Träger der Sozialhilfe zu benachrichtigen. Dieser soll dadurch in die Lage versetzt werden, rasch im Interesse des Mieters tätig zu werden. Der Verzug des Mieters muß indes nicht an seiner Mittellosigkeit liegen. Er kann sogar ein erhebliches Interesse daran haben, nicht als potentieller Sozialhilfeempfänger geführt zu werden.

Einen eingehenden Problemkatalog dieser Art habe ich dem Bundesminister der Justiz bereits im April 1981 zugesandt. Ich vertrete die Auffassung, daß eine Rechtsgrundlage — soweit nicht bereits vorhanden — jedenfalls dort zu fordern ist, wo befürchtet werden muß, daß durch die Mitteilung schutzwürdige Belange des einzelnen nachhaltig verletzt werden können. Wichtig ist es auch, die Übermittlungsvorgänge transparenter zu gestalten. Rührt doch das Unbehagen vieler Bürger beim Umgang mit der öffentlichen Verwaltung oftmals daher, daß diese über Kenntnisse verfügt, deren Herkunft den Betroffenen unbekannt ist. Ich habe außerdem angeregt, immer dann, wenn schutzwürdige Belange des einzelnen mit öffentlichen Interessen abgewogen werden müssen, den Richter entscheiden zu lassen. Schließlich sollte geprüft werden, welchen Umfang die Mitteilung jeweils haben muß, namentlich inwieweit es geboten ist, vollständige Ausfertigungen der gerichtlichen Entscheidungen zu übersenden.

Der Bundesminister der Justiz hat meine Überlegungen als „erwägenswert" bezeichnet und die Erörterung mit den Landesjustizverwaltungen sowie mit einer Reihe von Bundesressorts aufgenommen. Zu einzelnen Problemkreisen ist die Diskussion bereits vorangeschritten, so bezüglich

— der Unterrichtung der zuständigen konsularischen Vertretung bei Vernehmung von Ausländern an Bord ausländischer Schiffe bzw. von Besatzungsmitgliedern an Land (MiZi I 9) und bei Festnahmen (II 2) und

— der Benachrichtigung der für die leiblichen Eltern zuständigen Meldebehörde über Erlöschen des Verwandtschaftsverhältnisses bei Adoption (MiZi XIV 1).

Einer Mitteilung des Bundesministers der Justiz zufolge hat sich inzwischen die Mehrheit der Landesjustizverwaltungen für die ersatzlose Streichung der Mitteilungspflicht über Klagen auf Räumung von Wohnraum bei Zahlungsverzug des Mieters (MiZi IV 1) ausgesprochen.

Um die Überarbeitung der MiZi weiter zu fördern, halte ich an meiner Absicht fest, gemeinsam mit den Datenschutzbeauftragten der Länder Empfehlungen für Regelungen zu erarbeiten, die den Datenschutz stärker berücksichtigen. Dies soll im engen Kontakt mit denjenigen geschehen, die die Daten erhalten; dies sind in der Regel Verwaltungsbehörden in den Ländern, namentlich auf kommunaler Ebene, für die die Zuständigkeit der Landesbeauftragten gegeben ist.

2.2.5 Personenstandswesen

Auch in diesem Bereich gibt es Mitteilungspflichten, die auf Bewertungen beruhen, die heute nicht mehr allgemein geteilt werden. Beispiele hierfür sind:

— das Aufgebot, dessen Berechtigung ich bereits vor einiger Zeit (2. TB S. 19) in Zweifel gezogen habe,

— die Pflicht des Standesbeamten, bei Eintragungen über umherziehende Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten — eine pauschale Diskriminierung einer Personengruppe (4. TB S. 44).

Diese und weitere Beispiele sind Inhalt eines Problemkataloges, den ich zwecks datenschutzrechtlicher Überprüfung der vom Bundesminister des Innern erlassenen Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (DA) den für den Datenschutz in den Bundesländern Verantwortlichen zugesandt habe. Da ich zur täglichen Praxis der Standesbeamten weniger Zugang habe als meine Kollegen in den Ländern, bin ich auf deren Erfahrung und Mitwirkung angewiesen. Die Arbeit ist teilweise mit den Bemühungen um eine Überprüfung der Anordnung über Mitteilungen in Zivilsachen (MiZi) verknüpft und wird mit diesen Hand in Hand gehen. Ich begrüße, daß parallel zu meiner Initiative der Bundesminister des Innern Ende 1981 ebenfalls einen Ansatz zur datenschutzrechtlichen Überprüfung der Dienstanweisung entwickelt hat, und hoffe, daß sich bald konkrete Ergebnisse abzeichnen.

2.2.6 Mietpreisübersichten

Zu datenschutzrechtlichen Problemen im Bereich des Mietrechts habe ich bereits in früheren Tätigkeitsberichten Stellung genommen. Angesichts des

breiten Interesses der Öffentlichkeit an der Problematik von Mietpreisübersichten und einer zwischenzeitlichen Gesetzgebungsinitiative der Bundesregierung gehe ich hierauf erneut ein.

Die Bundesregierung hatte im Jahre 1982 den Entwurf eines Gesetzes über die Erstellung von Übersichten über die üblichen Entgelte für nicht preisgebundenen Wohnraum (Mietspiegelgesetz) eingebracht. Dem Gesetzentwurf ist jedoch im Oktober 1982 — nach vorhergehender Anrufung des Vermittlungsausschusses, der in seinem Beschluß eine Ablehnung vorgeschlagen hatte — durch den Bundesrat nicht zugestimmt worden. Bei weiteren Bemühungen um eine Regelung bzw. bei einer sich bildenden Verwaltungspraxis sollte auf die folgenden datenschutzrechtlichen Forderungen nicht verzichtet werden:

Unabhängig davon, ob eine Gemeinde sich selbst die Erstellung oder Festschreibung des Mietspiegels zur Aufgabe macht oder hiermit einen Dritten beauftragt, muß sichergestellt werden, daß bei der Verarbeitung der erhobenen Daten schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Es muß gewährleistet sein, daß Einzelangaben mit Namen und Anschrift nur zum Zwecke der Erstellung oder Fortschreibung des Mietspiegels verwendet werden. Die Gemeinden sollten verpflichtet sein, auf Verlangen Auskunft über die Ermittlung und Aufbereitung des ihrem Mietspiegel zugrundegelegten Datenmaterials zu erteilen. Dabei sollen Namen und Anschriften nicht mitgeteilt werden.

Eine enge Zweckbindung der in Mietpreisübersichten enthaltenen personenbezogenen Daten über Vermieter und Mieter halte ich wegen ihres hohen Sensibilitätsgrades für unverzichtbar. Solche Angaben lassen Schlüsse auf Einkommen und Lebensstil zu und berühren in der Regel schutzwürdige Belange der Betroffenen. Eine etwaige Bekanntgabe von Namen würde daher die Zustimmung sowohl des Vermieters als auch des Mieters erfordern.

In diesem Zusammenhang dürfte auch eine kürzlich ergangene Entscheidung des Bundesgerichtshofs (VIII ARZ 5/82) von Interesse sein, wonach bei einem Erhöhungsverlangen eines Vermieters zwar auf Vergleichswohnungen hingewiesen werden muß, die Namen der Vermieter und der Mieter dann aber nicht für erforderlich gehalten werden, wenn die Vergleichswohnung identifizierbar beschrieben worden ist.

2.2.7 Grundbuchwesen

Aufgrund von Bürgereingaben bin ich erneut darauf hingewiesen worden, daß schutzwürdige Belange berührt sein können, wenn Miteigentümer an einem gemeinsam genutzten Grundstück (z. B. Garagenflächen, gemeinsame Zugangswege) einen Grundbuchauszug benötigen. In einem solchen Auszug sind regelmäßig z. B. Name, Beruf, Geburtsdatum, Eigentumsanteil und Darlehensbelastungen der übrigen Miteigentümer enthalten. Ich habe bereits früher den Bundesminister der Justiz auf den datenschutzrechtlich bedenklichen Umfang eines solchen Grundbuchauszuges hingewiesen. Er hat seinerzeit erkennen lassen, daß meine Anregungen Anlaß zu neuen Überlegungen auf diesem Gebiet sind. Derzeit ist zwischen dem Bundesminister der Justiz und den Landesjustizverwaltungen ein Meinungsaustausch zu der Frage eingeleitet worden, ob eine Änderung oder Ergänzung der bestehenden grundbuchrechtlichen Vorschriften erwogen werden sollte.

2.2.8 Blutgruppengutachten

Der Bundesminister der Justiz hat mich im Jahre 1982 um eine Stellungnahme gebeten, ob datenschutzrechtliche Bedenken dagegen bestehen, daß Niederschriften über die Erstattung von Blutgruppengutachten von dem Gutachter an die ersuchenden Stellen weitergeleitet werden (vgl. Richtlinien des Bundesgesundheitsamts, Bundesgesundheitsblatt 1977 S. 326). Um die Zulässigkeit des Verfahrens vollständig beurteilen zu können, mußte ich in meine Prüfung auch die Erhebung der in die Niederschrift aufzunehmenden Angaben mit einbeziehen.

Ich habe empfohlen, dem Betroffenen, der beim Gutachter zu einer Blutentnahme und zur Aufnahme bestimmter Daten im Rahmen des hierfür notwendigen Identitätsnachweises erscheint, Aufklärung darüber zu geben, auf welchen Rechtsvorschriften der diesen Maßnahmen zugrundeliegende gerichtliche Beweisbeschluß beruht, und die Aufklärung in der vom Gutachter zu erstellenden Niederschrift zu vermerken.

Unverständlich ist mir, warum regelmäßig der Finger- bzw. Fußabdruck in die Niederschrift aufgenommen werden soll. Die Erforderlichkeit dieser Maßnahme ist im Regelfalle schon deshalb zweifelhaft, weil ein Gericht oder eine Behörde als Adressat des Gutachtens ohne zusätzliche gutachtliche Äußerung Dritter durchweg nicht in der Lage sein dürfte, den Abdruck zur Feststellung der Identität der begutachteten Person auszuwerten. Ein Finger- oder Fußabdruck sollte daher nur im Ausnahmefall nach vorheriger Prüfung durch den Auftraggeber des Gutachtens und entsprechendem ausdrücklichen Auftrag an den Gutachter verlangt werden.

Zweifel habe ich auch daran, ob der Identitätsnachweis erfordert, Nummer und Ausstellungsdatum des Passes bzw. Personalausweises in die Niederschrift aufzunehmen. Diese Daten können dem Auftraggeber nur dann dienlich sein, wenn er anderweitig über sie verfügt. Mir ist nicht ersichtlich, daß dies durchweg der Fall wäre.

Besondere Probleme ergeben sich bei der Datenübermittlung an ausländische Gerichte und Behörden: Eine Übermittlung ins Ausland muß dem Risiko Rechnung tragen, daß Identitätsdaten der genannten Art, namentlich Fingerabdrücke und Detailabgaben, über den Inhalt des Ausweises oder Passes, zu anderen als den Zwecken des Gutachtens genutzt werden könnten. Unter diesem Gesichtspunkt sollte die Rechtshilfe leistende Stelle im Einzelfall prüfen, ob internationale Rechtshilfe-

bestimmungen überhaupt eine Übermittlung der Niederschrift erlauben. Eine an ein ausländisches Gericht bzw. an eine ausländische Behörde zu übermittelnde Niederschrift sollte keinen Finger- bzw. Fußabdruck und keine Angaben über Nummer und Ausstellungsdatum von Paß bzw. Personalausweis des zu Begutachtenden enthalten. Ausnahmen sollten — so habe ich empfohlen — nur in besonderen Fällen nach eingehender Prüfung und entsprechender Entschließung des rechtshilfeleistenden deutschen Gerichts zulässig sein.

2.2.9 Überprüfung von Gerichtsbesuchern

Viele Bürger empfinden die Kontrollen, denen sich Besucher mancher Gerichte zu unterziehen haben, als eine ihre persönlichen Belange berührende Belastung und fragen zudem, ob sie mit dem Grundsatz der Öffentlichkeit der Verhandlung (§ 169 Gerichtsverfassungsgesetz) vereinbar sind. Die Eingabe eines Bürgers gab mir Gelegenheit, mit dem Bundesminister der Justiz und mit dem Präsidenten des Bundesgerichtshofs (BGH) das Verfahren der Überprüfung von Besuchern von Sitzungen des BGH zu untersuchen. Dabei ist nach meiner Beurteilung ein für alle Seiten akzeptabler Ausgleich zwischen den berechtigten Schutzinteressen des BGH, dem Prinzip der Öffentlichkeit der Verhandlung und den schutzwürdigen Belangen der Besucher gefunden worden:

Daß es sich beim BGH und bei der teilweise in demselben Gebäude untergebrachten Bundesanwaltschaft beim BGH um besonders sicherheitsempfindliche Dienststellen handelt, liegt auf der Hand. Die Eingangskontrolle muß sich konsequenterweise auf die Besucher der öffentlichen Sitzungen der Straf- und Zivilsenate erstrecken, um der nicht auszuschließenden Gefahr zu begegnen, daß sich potentielle Straftäter unter dem Vorwand, an öffentlichen Sitzungen teilnehmen zu wollen, Zugang zu dem Gelände und den Gebäuden des BGH und der Bundesanwaltschaft verschaffen.

Betreuer von Besuchergruppen werden nach Anmeldung gebeten, vor dem Besuchstermin eine Liste der Teilnehmer unter Angabe der Namen, der Anschriften, der Geburtsdaten und der Geburtsorte vorzulegen. Die Liste dient nach den Erklärungen des Präsidenten des BGH allein dem Zwecke, eine Personenüberprüfung bei der Datenstation im Landeskriminalamt Baden-Württemberg schon vor Eintreffen der Besucher durchzuführen und die Identifizierung der Besucher nach ihrem Eintreffen zu erleichtern und zu beschleunigen. Wie im Falle von Einzelbesuchern werden auch bei Besuchergruppen die Daten weder in der Datenstation des Landeskriminalamtes noch bei örtlichen Polizeidienststellen verwahrt oder gespeichert. Die Besucherlisten werden unmittelbar nach Beendigung des Besuches vernichtet.

Ich habe angeregt, die Mitglieder von Besuchergruppen bei Ausfüllung der Listen über deren Zweck und das Auswertungsverfahren zu unterrichten. Größere Transparenz des Verfahrens, Information auch darüber, daß die Besucherdaten nicht verwahrt oder gespeichert, die genannten Listen vielmehr unmittelbar nach Beendigung des Besuches vernichtet werden, sind geeignet, Mißtrauen und falsche Vorstellungen abzubauen und besseres Verständnis für notwendige Maßnahmen herzustellen. Wie mir der Bundesminister der Justiz inzwischen mitgeteilt hat, soll diesen Überlegungen nunmehr durch eine entsprechende Ergänzung der den Besucherformularen beigegebenen Erläuterungen Rechnung getragen werden.

2.3 Finanzverwaltung

2.3.1 Datenschutzkontrolle und Steuergeheimnis

Die Steuerverwaltungen geben den Datenschutzbeauftragten Auskünfte und Akteneinsicht zu Vorgängen, die unter das Steuergeheimnis fallen, bislang nur dann, wenn die Datenschutzbeauftragten aufgrund von Bürgereingaben tätig werden. Im übrigen ist die Finanzverwaltung des Bundes und der Länder der Meinung, daß die Datenschutzbeauftragten bei Kontrollen von Amts wegen keine Vorgänge zur Kenntnis nehmen dürften, die unter das Steuergeheimnis fallen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dieser Situation wiederholt, zuletzt im September 1982, befaßt. Im Einklang mit den Beschlüssen der Konferenz vertrete ich den Standpunkt, daß die Finanzbehörden den Datenschutzbeauftragten nicht unter Berufung auf das Steuergeheimnis (§ 30 der Abgabenordnung) Auskünfte und Einsicht in Akten verweigern dürfen. Der Auffassung der Finanzverwaltung ist entgegenzuhalten, daß § 30 der Abgabenordnung (AO) eine bereichsspezifische Geheimhaltungs- und Übermittlungsvorschrift ist. Nur insoweit geht sie, wie aus § 45 BDSG und den entsprechenden Vorschriften der Landesdatenschutzgesetze folgt, den Vorschriften der Datenschutzgesetze vor. Zur Datenschutzkontrolle sagt weder § 30 AO noch eine andere Vorschrift der AO etwas aus. Infolgedessen gelten für den Bereich der Steuerverwaltung uneingeschränkt

— § 19 Abs. 1 Satz 1 BDSG und die entsprechenden Vorschriften der Landesdatenschutzgesetze, wonach den Datenschutzbeauftragten auch die Kontrolle der Einhaltung anderer Vorschriften über den Datenschutz obliegt, und

— § 19 Abs. 3 BDSG und die entsprechenden Vorschriften der Landesdatenschutzgesetze über die Unterstützungs- und Auskunftspflicht der kontrollierten Behörden.

Es wäre unverständlich und insbesondere mit dem eindeutigen Wortlaut der Datenschutzgesetze nicht vereinbar, wenn dem gesetzlichen Kontrollorgan das Steuergeheimnis entgegengehalten werden könnte, dessen Einhaltung es gerade zu kontrollieren hat. § 30 Abs. 4 Nr. 2 AO erklärt die Durchbrechung des Steuergeheimnisses für zulässig, wenn sie durch Gesetz ausdrücklich zugelassen ist. § 19 Abs. 3 Satz 2 und 3 BDSG und die entsprechenden Regelungen der Landesdatenschutzgesetze sind ge-

setzliche Vorschriften, die eine Befugnis zur Offenbarung gegenüber den Datenschutzbeauftragten enthalten, indem sie die Finanzbehörde verpflichten, den Datenschutzbeauftragten Einsicht in alle Unterlagen und Akten, namentlich in die gespeicherten Daten zu gewähren sowie ihnen Auskunft zu geben. Eine im Rahmen der Datenschutzkontrolle notwendige Offenbarung steuerlicher Verhältnisse gegenüber den Datenschutzbeauftragten geschieht daher nicht unbefugt im Sinne von § 30 Abs. 2 AO. Die Datenschutzbeauftragten können — wie die Rechnungshöfe auch — ihrer gesetzlichen Kontrollaufgabe in der Finanzverwaltung nur nachkommen, wenn sie von ihren Kontrollbefugnissen uneingeschränkt Gebrauch machen können. Die Finanzbehörden müssen dadurch eine Erschwerung ihrer Arbeit nicht befürchten, da auch die Datenschutzbeauftragten die bei Kontrollen bekanntwerdenden Angelegenheiten nach § 18 Abs. 4 BDSG, den entsprechenden landesrechtlichen Regelungen bzw. der beamtenrechtlichen Schweigepflicht geheimzuhalten haben.

Im Einklang mit den Beschlüssen der Datenschutzkonferenz würde ich eine gesetzliche Klarstellung der Kontrollbefugnis der Datenschutzbeauftragten begrüßen (vgl. Nr. 6.2.8 dieses Berichts).

2.3.2 Im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung gespeicherte Daten

Die Datenschutzgesetze räumen dem Bürger grundsätzlich ein Recht ein, über die zu seiner Person gespeicherten Daten Auskunft zu verlangen. Nur in wenigen Ausnahmefällen legen die Datenschutzgesetze es in das pflichtgemäße Ermessen der Behörde, ob sie Auskunft erteilt. Ein solcher Fall ist gegeben, wenn Steuerbehörden (abgesehen von einer bayerischen Sonderregelung) personenbezogene Daten zur „Überwachung und Prüfung im Anwendungsbereich der Abgabenordnung" speichern. Bei ihrer übrigen Tätigkeit sind auch die Steuerbehörden zur Auskunftserteilung verpflichtet (und müssen ihre Dateien zum allgemeinen statt zum besonderen Datenschutzregister melden).

Die Tragweite dieser Ausnahmeregelung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mehrfach beschäftigt und war in deren Arbeitskreis „Steuerverwaltung" im August 1982 Gegenstand von Gesprächen mit Vertretern des Bundesministeriums der Finanzen. Die Ausnahmeregelung bezweckt, die Funktionsfähigkeit der Steuerbehörden sicherzustellen. Sie kann deshalb nur Platz greifen, soweit die Steuerverwaltungen ihren Auftrag nicht wahrnehmen könnten, wenn sie jedermann offenlegen müßten, welche Art von Daten sie speichern und an welche Stelle sie diese Daten regelmäßig übermitteln. Mit der Einschränkung des Auskunftsanspruchs durch die Formulierung „zur Überwachung und Prüfung im Anwendungsbereich der Abgabenordnung" sollte eine Ausforschung der Steuerbehörden verhindert werden.

Einigkeit mit dem Bundesministerium der Finanzen besteht darin, daß die Ausforschungsmöglichkeit der entscheidende Grund für die Regelung ist. Während das Ministerium ihn bislang jedoch für den „Anwendungsbereich der Abgabenordnung" schlechthin in Anspruch nimmt, ist nach Auffassung der Datenschutzbeauftragten zu differenzieren: Übereinstimmung besteht, daß die Daten der Betriebsprüfung, der Steuerfahndung, der Steueraufsicht und des Steuerstrafverfahrens im Rahmen der „Überwachung und Prüfung" geführt werden. Bei den meisten der sonstigen von den Steuerbehörden zum besonderen Register gemeldeten Dateien ist es dagegen nach Ansicht der Datenschutzkonferenz anders; hier ist eine Ausforschung in der Regel nicht möglich. Dies gilt insbesondere in den Fällen, in denen der Betroffene entweder die Daten selbst in seiner Steuererklärung der Steuerverwaltung mitgeteilt hat oder aus seinem Steuerbescheid entnehmen kann. Soweit mithin der Betroffene die Steuerverwaltung nicht ausforschen kann, sind uneingeschränkt Auskünfte zu erteilen und die Dateien zum allgemeinen Register zu melden.

Die Datenschutzbeauftragten haben das Angebot des Bundesministeriums der Finanzen begrüßt, ihnen eine Liste zu überlassen, in der zu jeder der in den einzelnen Dateien der Steuerverwaltung gespeicherten Datenarten näher begründet wird, warum das Datum „der Überwachung und Prüfung" dient. Ich hoffe, daß die weitere Diskussion eine Annäherung der Standpunkte bringt.

2.3.3 Kontrollmitteilungen

Kenntnisse über die für die Besteuerung von Steuerpflichtigen erheblichen Sachverhalte gewinnt die Finanzverwaltung nicht nur aufgrund der Auskunftspflicht der Steuerpflichtigen, sondern auch durch Inanspruchnahme Nichtbeteiligter zur Auskunftserteilung. Solche Auskünfte Nichtbeteiligter werden als Kontrollmitteilungen bezeichnet, wenn sie regelmäßig, d. h. ohne Einzelanforderung erteilt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dieser Problematik eingehend beschäftigt und in einem Beschluß vom September 1982 an die Finanz- und Steuerverwaltungen appelliert, Kontrollmitteilungen unter Beachtung des Grundsatzes der Verhältnismäßigkeit auf eine eindeutige Rechtsgrundlage zu stellen, sie dabei nur im unbedingt erforderlichen Umfang zuzulassen und die schutzwürdigen Belange der Betroffenen dadurch zu berücksichtigen, daß die Auskunft gebende Stelle oder Person die Betroffenen durch Übersendung einer Durchschrift der Mitteilung oder in anderer geeigneter Form unterrichtet.

Kontrollmitteilungen lassen sich weder aus den Besteuerungsgrundsätzen des § 85 der Abgabenordnung (AO), der lediglich eine Aufgabenzuweisungsnorm darstellt, noch — im öffentlichen Bereich — allein aus den Amtshilfevorschriften der §§ 111 ff. AO rechtfertigen. Die Amtshilfevorschriften enthalten lediglich Verfahrensregelungen und räumen keine materiell-rechtlichen Eingriffsbefugnisse ein. Auch § 93 AO stellt keine Rechtsgrundlage für Kontrollmitteilungen dar. Diese Vorschrift begründet

zwar eine Auskunftspflicht über für die Besteuerung des Steuerpflichtigen erhebliche Sachverhalte. Nichtbeteiligte dürfen aber nur im Einzelfall aufgrund eines konkreten Auskunftsersuchens in Anspruch genommen werden (§ 93 Abs. 2 Satz 1 AO); dabei ist sorgfältig zu prüfen, ob die Auskunft zur Feststellung des steuererheblichen Sachverhalts erforderlich ist (§ 93 Abs. 1 Satz 1 AO). In der Praxis werden aber häufig generelle Auskunftsersuchen ohne Bezug auf einen konkreten Einzelfall gestellt. Außerdem sind nach § 93 Abs. 1 Satz 3 AO zunächst die Steuerpflichtigen selbst zu befragen; Nichtbeteiligte sollen nur in Anspruch genommen werden, wenn die Sachverhaltsaufklärung durch die Beteiligten tatsächlich nicht zum Ziele führt oder keinen Erfolg verspricht. Auch diese Vorschrift wird häufig nicht in der gebotenen engen Auslegung gehandhabt. Da im Auskunftsersuchen steuerliche Verhältnisse des Betroffenen offenbart und dadurch dessen schutzwürdige Belange beeinträchtigt werden können, ist aus datenschutzrechtlicher Sicht ihre strenge Beachtung zu fordern.

2.3.4 Änderung der Abgabenordnung

Der Bundesminister der Finanzen hat Ende Oktober 1982 den Referentenentwurf eines Gesetzes zur Änderung der Abgabenordnung vorgelegt. Ich begrüße es, schon in diesem frühen Stadium beteiligt zu werden. In einer Reihe von Punkten muß ich auf datenschutzrechtliche Bedenken aufmerksam machen. Zwei Probleme hebe ich heraus:

Der Entwurf sieht in Ergänzung des § 16 der Abgabenordnung vor, Finanzbehörden im Verwaltungsverfahren in Steuersachen nicht als Dritte im Sinne des Bundesdatenschutzgesetzes und entsprechender landesrechtlicher Bestimmungen anzusehen, wenn Verwaltungstätigkeiten unterschiedlichen Finanzbehörden übertragen worden sind. Zur Begründung der geplanten Einfügung gibt der Entwurf an, ein ungehinderter Informationsaustausch zwischen den Finanzbehörden sei zur Erhaltung der Funktionsfähigkeit des Besteuerungsverfahrens notwendig. Einen Anhaltspunkt dafür, daß die Datenschutzgesetze den Informationsaustausch behinderten und dies gar in einer Weise, die die Funktionsfähigkeit des Besteuerungsverfahrens gefährde, bietet die Begründung dagegen nicht. Solcher Nachweis wird sich auch nicht erbringen lassen. Notwendige Datenübermittlungen zwischen Behörden werden durch die Übermittlungsvorschriften der Datenschutzgesetze keineswegs behindert. § 10 BDSG bzw. die vergleichbaren Vorschriften der Landesdatenschutzgesetze besagen, daß eine Übermittlung personenbezogener Daten an eine andere Behörde oder sonstige öffentliche Stelle zulässig ist, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Dies bedeutet: Einer Übermittlung der für die Aufgabenerfüllung der einzelnen Finanzbehörde erforderlichen Daten stehen Bestimmungen über den Datenschutz nicht im Wege. Der Datenschutz würde den Informationsaustausch zwischen den Finanzbehörden nur dann behindern, wenn man Daten übermitteln wollte, die für die Aufgabenerfüllung nicht erforderlich sind. Solchen Bestrebungen müßte ich entgegentreten.

Normadressat der genannten datenschutzrechtlichen Vorschriften ist die *einzelne* Behörde oder sonstige öffentliche Stelle als speichernde Stelle (§ 1 Abs. 2 Satz 1 Nr. 1 i. V. m. § 2 Abs. 3 Nr. 1 BDSG). Das Ziel das Datenschutzrechts, der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken, wäre wesentlich reduziert, wenn die Regelungen über die Datenübermittlung nur noch zwischen verschiedenen Verwaltungsbereichen anwendbar wären, innerhalb dieser Verwaltungsbereiche der Datenaustausch aber völlig freigegeben würde. Die Vorschrift des Entwurfs, die „im Verwaltungsverfahren in Steuersachen" unterschiedliche Finanzbehörden als eine Einheit ansieht und damit die Erforderlichkeitsprüfung der Datenübermittlung zu vermeiden sucht, wäre ein einschneidender Schritt in diese Richtung. Die geplante Ergänzung zu streichen, muß ich auch deshalb nachdrücklich raten, weil die Möglichkeit einer Nachahmung in anderen Bereichen (etwa im Sozialbereich, im Sicherheitsbereich) naheliegt und damit das Datenschutzrecht in seinem Grundbestand gefährdet wäre.

Ein weiterer wichtiger Gegenstand der Kritik ist die geplante Ergänzung des § 112 der Abgabenordnung dahin gehend, daß über Auskünfte im Einzelfall hinaus Auskünfte „allgemein" zum Gegenstand der Amtshilfe gemacht werden sollen. Die Ergänzung versucht zwar durch Schaffung einer Rechtsnorm das Bedenken auszuräumen, daß über den Einzelfall hinausgehende, an generelle Kriterien geknüpfte, d. h. regelmäßige Datenübermittlungen nicht auf ministerielle Erlasse gestützt werden können. Die Übermittlung personenbezogener Daten bedarf als grundrechtsrelevanter Eingriff einer Ermächtigungsnorm. Ein Amtshilfeersuchen bedeutet jedoch seinem Wesen nach nur ein Ersuchen um Hilfe im Einzelfall. Es darf nicht auf Dauer angelegt sein, etwa derart, daß die ersuchte Behörde ständig bestimmte Dienstgeschäfte für die auftraggebende Behörde durchführt. Gerade hierauf deutet aber die Entwurfsbegründung hin, die durch allgemeine Kriterien charakterisierte Sachverhalte wie „Bewillungen, ... Zahlungsvorgänge usw." nennt und damit nicht nur eine Vielzahl bereits entstandener Fälle umfaßt, sondern auch künftige, erst nach dem Amtshilfeersuchen entstehende Fälle einschließt.

Die beabsichtigte Ergänzung des § 112 erscheint zudem im Hinblick auf die im Rahmen des Entwurfes geplante Neufassung des § 116 der Abgabenordnung überflüssig. Mit der dort vorgesehenen Verpflichtung von Gerichten und Behörden, steuerrelevante Tatsachen mitzuteilen, wird m. E. ein Informationsrahmen geschaffen, der eine zusätzliche und in ihren Grenzen zweifelhafte Ausweitung des § 112 AO entbehrlich macht.

Schließlich hätte eine Ausdehnung des Begriffes der Amtshilfe Wirkungen, die über den Bereich des Finanzwesens hinausgehen. Sie stünde im Gegensatz zu anderen den Begriff der Amtshilfe verwendenden Gesetzen — so besonders das Verwaltungs-

verfahrensgesetz (§§ 4 und 5) — und würde die Einheitlichkeit des Begriffes der Amtshilfe beseitigen.

Vor dem Hintergrund vorstehender Ausführungen zur Frage der Kontrollmitteilungen verdienen außerdem solche Regelungen des Änderungsentwurfs besondere Aufmerksamkeit, die den Behörden und Gerichten die Pflicht auferlegen, im Rahmen einer Art und Umfang regelnden Rechtsverordnung den Finanzbehörden Tatsachen mitzuteilen, die für die Besteuerung und ihre Durchführung von Bedeutung sein können (§ 116 des Entwurfs), sowie als Gegenstück hierzu den Finanzbehörden das Recht gewähren, von Steuerpflichtigen Auskunft über die in § 160 der Abgabenordnung genannten Sachverhalte auch außerhalb ihres Besteuerungsverfahrens zu verlangen (§ 93 des Entwurfs). Dort ist das angestrebte Ziel, sicherzustellen, daß im privaten Bereich Einkünfte aus Nebentätigkeiten, Zahlungsrückflüsse, Rabattgewährungen u. ä. versteuert werden, hier, daß aus öffentlichen Kassen geleistete Zahlungen von den Empfängern vollständig versteuert werden.

Die Datenschutz-Kontrollinstanzen werden diesem Anliegen der Finanzbehörden nicht im Wege stehen. Nach ihrer Auffassung sollte jedoch bei der Formulierung des vorliegenden Änderungsentwurfes wie bei der Durchführung des Gesetzes darauf geachtet werden, daß Nichtbeteiligte, d. h. andere als die Steuerpflichtigen selbst, durch Auskunftsersuchen nicht über den unbedingt erforderlichen Umfang hinaus in Anspruch genommen werden. Diese Forderung der Datenschutzbeauftragten resultiert aus dem Eingriffscharakter steuerbehördlicher Aufklärungsmaßnahmen und stützt sich auf das in § 93 Abs. 1 Satz 3 der Abgabenordnung verankerte sogenannte Subsidiaritätsprinzip, zuerst den Steuerpflichtigen selbst zur Auskunftserteilung heranzuziehen und Dritte nur dann zu befragen, „wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht".

2.3.5 Datenübermittlung der Finanzbehörden an Drittschuldner

Unter der Überschrift „Einblick vom Fiskus" wurde in einem Zeitungsartikel als Fall, der „dem Anliegen der Datenschützer Berechtigung" verleihe, folgendes geschildert: Zur Durchsetzung von Steuerforderungen gegen einen Mietshauseigentümer habe das Finanzamt die Mieten von -zig Mietern gepfändet und diesen mitgeteilt, sie müßten an den Fiskus zahlen, weil der Vermieter folgende Steuerschulden habe — es folgte sodann eine Aufzählung von fünf Steuerarten: Einkommensteuer, Kirchensteuer für eine bestimmte Konfession, Vermögensteuer usw.

Der Artikel geht zutreffend davon aus, daß es sich insoweit um personenbezogene Daten handelt, als es um die Spezifizierung der Art der Steuerschuld geht. Ich habe Zweifel, ob die Unterrichtung von Drittschuldnern eine derartige Spezifizierung der Entstehungsgründe der Forderung zu deren Durchsetzung erfordert. Ich habe daher den Bundesminister der Finanzen um eine Stellungnahme gebeten, ob — wie der Artikel annimmt — die Abgabenordnung oder andere Gesetze derart detaillierte Einblicke in die Verhältnisse des Steuerschuldners wirklich erzwingen.

Der Minister hat auf § 260 der Abgabenordnung hingewiesen, der verlangt, im Vollstreckungsauftrag bzw. in der Pfändungsverfügung den Schuldgrund anzugeben. Zahlungen des Drittschuldners dürften nur auf die zu vollstreckende Forderung und nicht etwa auch auf andere Schulden des Vollstreckungsschuldners verrechnet werden. Ich bin der Auffassung, daß dies auch ohne Mitteilung der Entstehungsgründe der Forderung an den Drittschuldner gewährleistet werden kann. Ich habe feststellen können, daß meine Überlegungen von vielen Bürgern besonders in der Wirtschaft geteilt werden, und betrachte die Erörterung noch nicht als abgeschlossen.

2.4 Personalwesen

2.4.1 Allgemeines

Im Jahre 1980 hatte ich als einen Schwerpunkt meiner Arbeit die Beurteilung von Personalinformationssystemen gewählt. Die öffentliche Diskussion um den Einsatz derartiger Systeme im Bereich der privaten Wirtschaft hatte meine Sorge verstärkt, hier könne die Situation entstehen, daß Datenverarbeitungssysteme bei der Entscheidung über Menschen einen zu weitgehenden Einfluß gewinnen. Schon die Personalakte bildet den Betroffenen nur unvollkommen ab. Jeder Mensch hat Eigenschaften, die nicht exakt beschreibbar oder gar meßbar sind. Diese Eigenschaften können aber für eine qualifizierte Personalentscheidung durchaus von Bedeutung sein. Dafür ist es wichtig, den Betroffenen persönlich zu kennen.

Wird nun der Inhalt einer Akte formalisiert, um ihn in einer elektronischen Datei zu speichern, so wird die Beschreibung des Betroffenen noch mehr reduziert und noch weniger präzise; das Bild vergröbert sich. So ist nicht auszuschließen, daß bei der Verarbeitung dieser Daten mittels Programm falsche Entscheidungen getroffen werden, weil die Formalisierung der Daten und der Verarbeitungsregeln den tatsächlichen Gegebenheiten des einzelnen Betroffenen nicht gerecht werden konnte. Daher muß nachdrücklich gefordert werden und sichergestellt sein, daß die Funktion von Personalinformationssystemen auf Entscheidungs*hilfen* beschränkt wird; die Entscheidung selbst darf nicht dem System überlassen werden.

Dem wird oft entgegengehalten, eine Entscheidung durch den Algorithmus eines EDV-Systems sei objektiv. Darauf allein kann es jedoch nicht ankom-

men. Auch ein guter Personalsachbearbeiter oder Vorgesetzter urteilt objektiv. Er kann jedoch im Gegensatz zu einem elektronischen System weitere Aspekte und Unvorhergesehenes mit berücksichtigen.

Es zeigte sich, daß Personalinformationssysteme in der Bundesverwaltung noch nicht so häufig sind, wie dies für den Privatbereich bekannt ist. Von den näher untersuchten Systemen erwies sich lediglich das Personalführungs- und Informationssystem Soldaten (PERFIS) als Personalinformationssystem im eigentlichen Sinne. Ich habe deshalb dort 1980 eine Kontrolle durchführen lassen, die 1982 fortgesetzt wurde. Die Kontrolle ist jetzt abgeschlossen (s. u. Nr. 2.4.5). Bei Bundesbahn und Bundespost bestehende Systeme bleiben noch zu kontrollieren.

Meine Sorge, in Personalinformationssystemen würden Personalentscheidungen maschinell getroffen, hat sich im System PERFIS nicht bestätigt. Zwar werden Ergebnisse von Beurteilungen der Mitarbeiter gespeichert und Reihungslisten (Vorschlagslisten für Beförderungen) maschinell erstellt; der Personalsachbearbeiter kann jedoch in begründeten Fällen davon abweichen.

Bereits in meinem Zweiten Tätigkeitsbericht (S. 24) habe ich darauf hingewiesen, daß zu prüfen sei, ob nicht im Bereich des Personalvertretungs-/Betriebsverfassungsrechts bereichsspezifische Regelungen notwendig seien. Die betrieblichen Informationsbeziehungen sind so zu gestalten, daß die automatische Datenverarbeitung oder das Datenschutzrecht nicht zu einer Verschiebung des Kräfteverhältnisses führen. Eine Mitgestaltung der Personalräte hinsichtlich des Inhalts und der Nutzung von Personalinformationssystemen ist unverzichtbar.

Daten, die zu Abrechnungszwecken erhoben werden oder der Effizienzkontrolle von EDV-Systemen dienen sollen, eignen sich auch zur Kontrolle der Mitarbeiter und werden in von mir festgestellten Fällen auch dazu benutzt. Ein Beispiel dafür ist die Entwicklung und Einführung von Dialogsystemen. Werden die zu bearbeitenden Vorgänge durch den Sachbearbeiter im unmittelbaren Dialog mit einem EDV-System abgewickelt, läßt sich im System unschwer feststellen, wie viele Fälle jeder Sachbearbeiter in einem bestimmten Zeitraum abgewickelt hat, wie viele Fehler er dabei gemacht hat usw. Eine solche Auswertung ist sicherlich auch sinnvoll, um festzustellen, ob ein System angenommen und wie es genutzt wird. Dies gilt besonders dann, wenn ein System gerade eingeführt wird. Ich bezweifle jedoch, daß für diesen Zweck tatsächlich eine personenbezogene Aufzeichnung erforderlich ist. Meines Erachtens reicht eine Aufzeichnung, die keine Rückschlüsse auf die Arbeitsleistung des einzelnen Sachbearbeiters zuläßt, völlig aus, um die Effizienz des Systems zu beurteilen. Die Arbeitsleistung des mit dem System arbeitenden Sachbearbeiters sollte dagegen in erster Linie von seinem Vorgesetzten beurteilt werden.

2.4.2 Konventionelle Verfahren

In meine Kontrollen habe ich auch häufig die Führung der Personalakten einbezogen und bin dabei auf vielerlei Probleme und Unsicherheiten gestoßen. In letzter Zeit ist vereinzelt auch meine Kontrollkompetenz im Personalwesen in Frage gestellt worden. Dazu beziehe ich mich auf meine Ausführungen in meinem Dritten Tätigkeitsbericht, S. 57 f. Gemäß § 19 Abs. 1 BDSG habe ich die Pflicht, nicht nur die Einhaltung der Vorschriften des BDSG, sondern auch die der anderen Vorschriften über den Datenschutz einschließlich der Verwaltungsvorschriften zu kontrollieren. Kontrollmaßstab für den Bereich des Personalwesens sind danach die Vorschriften des Beamten- und Tarifrechts zum Personalaktenwesen. Selbstverständlich sind dabei auch die Grundrechte, die unmittelbar geltendes Recht sind, aber auch die durch die höchstrichterliche Rechtsprechung erarbeiteten Rechtsgrundsätze zu berücksichtigen.

Die gesetzlichen Vorschriften des Personalaktenwesens sind allerdings sehr dürftig. Sowohl das Beamtenrecht (§ 90 BBG) als auch das Tarifrecht des öffentlichen Dienstes (§ 13 BAT, § 13 a MTB II) enthalten neben dem Vollständigkeitsgebot nur Regelungen über das Einsichtsrecht des Beschäftigten und das Verfahren der Aufnahme von Schriftstükken in die Personalakte, wenn sie für den Beschäftigten einen negativen Inhalt haben. Die Rechtsprechung hat die genannten Vorschriften konkretisiert und Grundsätze für die Führung von Personalakten und den Umgang mit den darin enthaltenen Informationen entwickelt.

Wird ein Sachverhalt an einer solchen anderen Vorschrift über den Datenschutz gemessen, so kommt es für meine Kontrollbefugnis nicht darauf an, ob die personenbezogenen Daten in der Form einer Datei verarbeitet werden. Die Verarbeitungsform der Datei kann hier schon deshalb nicht von Belang sein, weil die bereichsspezifischen Datenschutzvorschriften regelmäßig nicht auf eine Gefährdung durch eine besondere Form der Verarbeitung abstellen, sondern auf die Gefährdung wegen der Sensivität der Daten und ihres Verwendungszusammenhangs. Eine Beschränkung der Datenschutzkontrolle auf Dateien — bei Datenschutzvorschriften, die eine solche Einschränkung nicht kennen — wäre auch für den hilfesuchenden Bürger unverständlich.

Eine umfassende Unterrichtungsmöglichkeit ist auch Voraussetzung für die Wahrnehmung der mir vom Gesetzgeber zugewiesenen Aufgabe, Empfehlungen zur Verbesserung des Datenschutzes zu geben. Wird mir diese Unterrichtungsmöglichkeit nur noch dann zugestanden, wenn Personaldaten in Dateien verarbeitet wrden, so sehe ich mich außerstande, Empfehlungen zur Verbesserung des Datenschutzes bei der manuellen Personaldatenverarbeitung zu geben, die nicht nur rein theoretisch und abstrakt sind, sondern sich an den Bedürfnissen und Verhältnissen der Praxis orientieren.

Personalaktengeheimnis

Die Personalakte im materiellen Sinne — d. h. alle die Personalangelegenheiten des Beamten betreffenden Unterlagen und Vorgänge ohne Rücksicht darauf, wo sie vermerkt sind oder aufbewahrt werden — unterliegt schon als Behördenakte und insbesondere im Interesse des Beamten nach einem hergebrachten Grundsatz des Berufsbeamtentums der Dienstverschwiegenheit. Dies gilt ebenso für Angestellte und Lohnempfänger. Das Personalaktengeheimnis wirkt stärker als das allgemeine Amtsgeheimnis (§§ 61 BBG, 39 BRRG). Mitteilungen im dienstlichen Verkehr, insbesondere im Wege der Amtshilfe, dürfen bei Personaldaten weder innerhalb einer Behörde noch im Verkehr der Behörden untereinander beliebig erfolgen. Das Bundesverwaltungsgericht hat entschieden, daß Personalakten — was auch in der Verwaltungspraxis allgemein anerkannt sei und durch zahlreiche Regelungen bestätigt werde (vgl. z. B. § 68 Abs. 2 Satz 3 BPersVG) — ohne Einwilligung des Beamten grundsätzlich nur von einem eng begrenzten Personenkreis mit besonderer dienstlicher Verantwortung (Personalreferent, Behördenleiter) eingesehen werden dürfen; sie genießen sowohl im dienstlichen Interesse als auch im schutzwürdigen persönlich-privaten Interesse des Beamten einen besonderen Vertrauensschutz, der sich auch auf den Verkehr der Behörden untereinander erstreckt. Personalakten gehören grundsätzlich zu den Vorgängen, die gemäß § 99 Abs. 1 Satz 2 VwGO „ihrem Wesen nach geheimgehalten werden müssen" (BVerwGE 19, 179, 185).

Aufgrund von Eingaben, aber auch im Rahmen von Kontrollen mußte ich feststellen, daß dieser Grundsatz nicht immer eingehalten wird. In Gesprächen bei geprüften Behörden konnte ich feststellen, daß das Einsichtsrecht häufig nicht nur dem betroffenen Beschäftigten und den an Personalentscheidungen direkt Beteiligten vorbehalten wird, sondern daß auch unmittelbare und mittelbare Fachvorgesetzte Einsicht in Personalakten erhalten. Dies ist nach den oben angeführten Entscheidungen grundsätzlich unzulässig. Ich begrüße deshalb Regelungen, wie sie z. B. der Bundesminister für das Post- und Fernmeldewesen (BMP) in seinen „Anweisungen für die Führung und Verwaltung von Personalakten des Beamten" (Amtsbl. 1980, S. 391) herausgegeben hat, in denen ausgeführt wird, daß „Personalakten und Personalpapiere nur den Dienstvorgesetzten, den Leitern der Personalabteilungen und den mit der Vorbereitung und Bearbeitung von Personalangelegenheiten beauftragten Beschäftigten zugänglich sein dürfen". Noch enger faßt der nordrhein-westfälische Innenminister den Kreis der Zugriffsberechtigten. Während der BMP auch den an der Vorbereitung von Personalentscheidungen Beteiligten ein Einsichtsrecht gewährt, führt der nordrhein-westfälische Innenminister in seinen Verwaltungsvorschriften zu § 102 Landesbeamtengesetz — NRW aus, daß neben dem Behördenleiter und seinem ständigen Vertreter nur der mit der Bearbeitung von Personalangelegenheiten beauftragte Bedienstete die Personalakte einsehen darf. Ich neige der Auffassung zu, daß dem Fachvorgesetzten nur ausnahmsweise ein Recht auf Einsicht in die Personalakte zugebilligt werden kann, dann nämlich, wenn er an der Personalentscheidung beteiligt ist, z. B. indem er aus dem Kreis seiner Beschäftigten eine Vorauswahl bei der Beförderung treffen muß und dem Dienstvorgesetzten einen oder nur wenige Beschäftigte zur Beförderung vorschlagen soll. Der Fachvorgesetzte darf aber nur die Unterlagen einsehen, die er für seine Mitwirkung an der Entscheidung benötigt, keinesfalls die vollständige Personalakte. Im Zweifelsfall sollte die Zustimmung des Betroffenen eingeholt werden.

Vollständigkeitsgebot

Mehrere Eingaben aus dem Bereich des Personalwesens befaßten sich mit dem Gebot der Vollständigkeit der Personalakte. Gemäß § 90 BBG, § 13 BAT, § 13 a MTB II hat der Beschäftigte ein Recht auf Einsichtnahme in seine *vollständigen* Personalakten. Nach diesem Gebot gehören alle auf die persönlichen und dienstlichen Verhältnisse des Beschäftigten bezogenen Urkunden und aktenmäßig festgehaltenen Vorgänge zu den Personalakten (BVerwG, ZBR 1965, 215) — ohne Rücksicht darauf, ob sie in der formellen Personalakte aufbewahrt werden oder nicht. Bei der Prüfung der Eingaben mußte ich jedoch mehrfach feststellen, daß Behörden Schriftstücke, die den Beschäftigten in seinen persönlichen oder dienstlichen Verhältnissen betreffen, nicht in die Personalakte heften, sondern sie in besonderen Nebenakten oder in Fachakten ablegen (siehe auch 4. TB S. 12). In einem Fall lag dem Fachvorgesetzten ein Schriftstück des Dienststellenleiters vor, aus dem sich Einzelheiten zu einer vermeintlichen psychischen Krankheit einer Beschäftigten ergaben. Weder vom Inhalt noch von der Existenz des Schriftstückes hatte die Beschäftigte Kenntnis. Als sie hiervon erfuhr und in ihre Personalakte Einblick nahm, fand sie darin keine Hinweise auf dieses Schreiben. Es hätte entweder sofort vernichtet oder zur Personalakte genommen werden müssen, weil es die Beschäftigte in ihren persönlichen und dienstlichen Verhältnissen berührte. Ich habe diesen Vorfall beanstandet.

Personalaktenähnliche Vorgänge

Bei Kontrollen konnte ich wiederholt feststellen, daß es neben den Personalakten in der Personalverwaltung auch personalaktenähnliche Vorgänge in Fachabteilungen oder Außenstellen der Behörden gibt. In diesen Akten waren Unterlagen zu finden, z. B. Entwürfe oder Mehrfertigungen von Beurteilungen, Schriftstücke mit Aussagen über Leistungsfähigkeit oder Leistungsschwächen einzelner Mitarbeiter, die eindeutig in die Personalakte gehörten oder hätten vernichtet werden müssen.

Über die Frage, wer personalaktenführende Stelle ist, treffen weder das Beamtenrecht noch das Recht der Angestellten und Arbeiter abschließende Feststellungen. Jedoch gibt die Festlegung der Aufgaben des Dienstvorgesetzten (§ 3 Abs. 2 Satz 1 BBG) hier weiteren Aufschluß. Dienstvorgesetzter ist, wer für beamtenrechtliche Entscheidungen über die

persönlichen Angelegenheiten der ihm nachgeordneten Beamten zuständig ist. Personalaktenführende Stelle kann daher nur ein Dienstvorgesetzter sein. Welcher Dienstvorgesetzte dies ist, bestimmt sich nach der Organisation der Verwaltung. Die Personalakten sind in jedem Fall nur bei einer Stelle zu führen (s. Plog-Wiedow, Komm. z. BBG, § 90 Anm. 6); andere Stellen dürfen auch personalaktenähnliche Unterlagen nicht führen, es sei denn, daß sie sie zur rechtmäßigen Aufgabenerfüllung oder aus organisatorischen Gründen benötigen. So muß eine Fachabteilung aus den eigenen Unterlagen erkennen können, welche Beschäftigten welcher Besoldungs-/Vergütungs- oder Lohngruppe ihr zur Dienstleistung auf welchen Dienstposten zugewiesen worden sind. Ist die Fachabteilung an der Erstellung von personalaktenwürdigen Schriftstükken beteiligt, wie das z. B. bei der Beurteilung der Fall ist, so dürfen diese Schriftstücke nicht, auch nicht in Form von Entwürfen oder Durchschriften, in der Fachabteilung verbleiben, sondern müssen entweder vernichtet oder der personalaktenführenden Stelle abgegeben werden. Dies ist auch in den meisten Beurteilungsrichtlinien so vorgeschrieben.

Anhörung des Beschäftigten vor Aufnahme von Schriftstücken in die Personalakte

Das Beamtenrecht und das Recht der Arbeitnehmer des öffentlichen Dienstes schreiben vor, daß der Beschäftigte vor Aufnahme eines Schriftstükkes in die Personalakte anzuhören ist, wenn dieses Beschwerden oder Behauptungen tatsächlicher Art enthält, die für ihn ungünstig sind oder ihm nachteilig werden können (§ 90 Satz 2 BBG, § 13 Abs. 2 BAT, § 13 a Abs. 2 MTB II). Dabei kommt es nicht darauf an, ob der Dienstherr/Arbeitgeber aus den Vorgängen für den Beschäftigten nachteilige Schlußfolgerungen zieht, sondern darauf, ob bei objektiver Betrachtungsweise irgendein Leser der Personalakte daraus für den Beschäftigten Nachteiliges folgern könnte. Obwohl hier die Rechtslage eindeutig ist, mußte ich im Rahmen mehrerer Eingaben feststellen, daß dieser Grundsatz mißachtet wurde.

2.4.3 Zugangskontrolle

In einer Vielzahl von Behörden und sonstigen Stellen meines Zuständigkeitsbereichs sind in den letzten Jahren Zugangskontrollsysteme installiert worden. Solche Systeme dienen üblicherweise der im BDSG geforderten Zugangskontrolle und häufig auch der Gleitzeiterfassung.

Je nach technischer Leistungsfähigkeit solcher Systeme kann so aufgezeichnet werden, wann ein Mitarbeiter ein Gebäude, einen Gebäudeteil oder einen Arbeitsraum betritt und verläßt. Es entsteht somit ein genaues Bild seines Zeitverhaltens an der Arbeitsstätte. Diese Daten könnten zweckentfremdet genutzt werden. Sie könnten zu einer so eingreifenden Kontrolle von Mitarbeitern verwendet werden, daß es zu Störungen des Arbeitsfriedens kommen kann.

Diese Gefahr vergrößert sich noch, wenn die Daten mit weiteren Personaldaten kombiniert werden oder in einer Datei zusammen mit vielen anderen Personaldaten gespeichert werden. Die Daten würden dann aus dem ursprünglichen Zusammenhang gelöst, gegebenenfalls neu interpretiert und zur Beurteilung oder zur Entscheidung über einen anderen Einsatz eines Mitarbeiters herangezogen werden können.

Wo der Einsatz von Zugangskontrollsystemen unumgänglich ist, kommt es darauf an, bei der Einführung solcher Systeme in Vereinbarungen mit den Personalvertretungen festzulegen, welche Daten erfaßt werden und wem sie zur Verfügung stehen sollen, welchen Zwecken sie dienen und wann sie gelöscht werden sollen. Ich werde im Rahmen meiner Kontrollen darauf achten, daß diesen Forderungen entsprochen wird.

2.4.4 Telefonkontrolle

Im Bereich der Bundesverwaltung ist bei *dienstlicher* Benutzung dienstlicher Fernsprecheinrichtungen die Aufzeichnung der Rufnummern von Gesprächsteilnehmern in Nr. 9 der Dienstanschlußvorschriften — DAV — des Bundesministers der Finanzen vom 1. Juni 1976 (Allgemeine Verwaltungsvorschrift für die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Deutschen Bundespost, Ministerialblatt des BMF und des BMWi 1976, S. 487) vorgeschrieben. Für eine Bundesgrenzschutzabteilung hat — über diese Vorschriften hinausgehend — der Dienststellenleiter angeordnet, außer der Zielnummer zum Nachweis abgehender Gespräche auch noch den Namen des angerufenen Gesprächsteilnehmers anzugeben.

In einer Reihe von Eingaben namentlich von Personalvertretungen wird die Rechtmäßigkeit dieses Verfahrens in Frage gestellt. So habe eine Verwaltungsstelle jüngst einem Personalrat die Frage vorgehalten, warum er denn so oft mit der Gewerkschaft telefoniert habe. Die Kritik richtet sich besonders gegen die Auffassung der Bundesminister des Innern und der Finanzen, das Verfahren der Aufzeichnung von Zielnummern müsse auch für Gespräche der Mitglieder von Personalvertretungen, von Geistlichen und von Ärzten gelten.

Ich habe mich zu dieser Problematik bereits in meinen früheren Tätigkeitsberichten (3. TB S. 28 f., 4. TB S. 39 f.) geäußert und gegenüber dem Bundesminister der Finanzen, dem Bundesminister des Innern und den übrigen betroffenen Bundesbehörden Bedenken gegen die Aufzeichnung der Zielnummern geltend gemacht. Bei der datenschutzrechtlichen Prüfung der DAV ist zu unterscheiden zwischen Gesprächen des Personalrats und anderer Einrichtungen, die eine besondere Vertrauensstellung genießen und besonderen Schweigepflichten unterliegen, z. B. des ärztlichen und sozialen Dienstes, und solchen „allgemeinen" Fällen von Dienstgesprächen, wo derartige Besonderheiten nicht vorliegen.

Nach meinen bisherigen Feststellungen sollen die Aufzeichnungen den Zwecken der Dienstaufsicht, der Wirtschaftlichkeitskontrolle (Verhinderung übermäßigen Gebrauchs) und der Mißbrauchskontrolle (Ausschluß von Privatgesprächen als vorgebliche Dienstgespräche) dienen. Es kann für die hier zu entscheidende Frage dahinstehen, ob man der datenschutzrechtlichen Prüfung § 9 Abs. 1 BDSG zugrunde legt oder das Problem dem Dienstrecht zuordnet und deshalb von § 23 Abs. 1 i. V. m. § 7 Abs. 3 BDSG ausgeht.

Entscheidendes Kriterium ist in jedem Falle die Erforderlichkeit der Speicherung. Ich möchte diese nicht von vornherein bestreiten, räume vielmehr ein, daß die Speicherung der Zielnummer von Dienstgesprächen dem Einstieg in eine schnelle überschlägige Prüfung dienen kann, die allenfalls bei auffälligen Angaben zu einer intensiveren Untersuchung z. B. anhand der Akten führt.

Die Bundesminister der Finanzen und des Innern haben mir aber trotz mehrfacher Aufforderung immer noch keine ausreichenden Informationen darüber gegeben, inwieweit Zielnummern-Aufzeichnungen auch tatsächlich — zumindest stichprobenweise — ausgewertet werden, sondern im wesentlichen bloß die Behauptung wiederholt, Kontrollen seien notwendig. Werden die Aufzeichnungen tatsächlich nicht ausgewertet, so wird man die Erforderlichkeit verneinen müssen.

Besonders bedenklich ist m. E. die Aufzeichnung der Zielnummern bei Gesprächen des Personalrates oder anderer Einrichtungen in besonderer Vertrauensstellung und mit besonderen Schweigepflichten. Gespräche dieser Stellen dürfen hinsichtlich ihrer Registrierung nicht denselben Anforderungen unterstellt werden wie die der übrigen Beschäftigten. Zwar muß die Dienststelle auch gegenüber dem Personalrat auf die wirtschaftliche und sparsame Verwendung der Mittel Einfluß nehmen können. Hierdurch darf aber dessen Unabhängigkeit nicht beeinträchtigt werden. Eine solche Beeinträchtigung ist jedoch zu befürchten, wenn die Dienststelle ohne Einschaltung des Personalrates kontrollieren kann, mit wem dieser Kontakte hat. Die Dienststelle kann die Zahl der Gespräche registrieren, deren Notwendigkeit m. E. aber nur gemeinsam mit dem Personalrat prüfen und eine Erfassung von Zielnummern nur mit dessen Einvernehmen anordnen.

Die von den genannten Bundesressorts vertretene Auffassung, der Personalrat habe kein Mitbestimmungsrecht bei der Frage der Erforderlichkeit und des Umfanges der zu führenden Nachweise, teile ich nicht, möchte eine Überprüfung dieser Frage aber den dafür zuständigen Stellen überlasssen.

Akzeptable Lösungen werden sich m. E. nur unter Berücksichtigung der Besonderheiten und speziellen Aufgaben des jeweiligen Dienstbereiches finden lassen. Meine Absicht ist es nicht, perfektionistische Lösungsmöglichkeiten für alle Dienstbereiche des Bundes anzubieten. Vielmehr geht es mir darum, Behörden und Bedienstete und deren Personalvertretungen gleichermaßen für die Problematik zu sensibilisieren und zu geeigneten Dienstvereinbarungen zu ermutigen. Auch ein Urteil des Landesarbeitsgerichtes Frankfurt, das die Klage eines Personalratsmitglieds mit der Begründung zurückgewiesen hat, der Personalrat habe das Verfahren der Registrierung von Anfang an gekannt und niemals beanstandet (Urteil vom 27. August 1981, nur unvollständig abgedruckt in MDR 1982, S. 82), muß m. E. als Aufforderung an den Personalrat verstanden werden, seine Handlungsmöglichkeiten auszuschöpfen.

Wie ich schon in meinen früheren Tätigkeitsberichten (a. a. O.) ausgeführt habe, bestehen Bedenken erst recht gegen die Aufzeichnung von Zielnummern bei *privaten* Telefongesprächen von Dienstapparaten aus. Nach meinen Erkenntnissen ist es in der Regel nicht erforderlich, die Zielnummern festzuhalten. Ausnahmen gelten dann, wenn der Beschäftigte selbst ein Interesse an detaillierterer Abrechnung äußert, sei es weil mehrere Bedienstete denselben Apparat benutzen und deshalb die Zuordnung einzelner Gespräche erschwert ist, sei es weil etwa entstandene Meinungsverschiedenheiten zwischen Dienststelle und Bedienstetem über die Gebührenabrechnung eine (befristete) detailliertere Abrechnung nahelegen.

Um das Problem zu entschärfen, sollten praktische Lösungswege gesucht werden. So würde es einen Fortschritt darstellen, wenn die benutzten Verfahren und Techniken der Aufzeichnung und Auswertung allgemein den Betroffenen bekanntgemacht würden. Ferner sollte dafür gesorgt werden, daß alle aufgezeichneten Daten auf allen Datenträgern nach Ausdruck von Listen und Abrechnungen gelöscht werden. Bemerkenswert erscheint mir auch ein im Dritten Tätigkeitsbericht des nordrhein-westfälischen Landesbeauftragten für den Datenschutz (S. 71) enthaltener Vorschlag, bei Privatgesprächen entweder auf eine Speicherung der Zielnummern ganz zu verzichten oder aber bei der Erfassung dieser Daten die letzten Ziffern wegzulassen.

Hersteller von Zusatzeinrichtungen zum Telefon sind weiterhin aufgerufen, zu dieser Diskussion beizutragen und technische Lösungen zu entwickeln, die die individuellen Interessen der Beteiligten in bestmöglichem Maße berücksichtigen.

Der Bundesminister der Finanzen und der Bundesminister des Innern haben bislang keine Bereitschaft gezeigt, auf solche Vorschläge einzugehen. Sie begründen ihre Ablehnung für Dienstgespräche mit dem Hinweis, die Dienstaufsicht umfasse die Befugnis des Dienstherrn, sich einen Einblick in jede dienstliche Tätigkeit des Beamten zu verschaffen. Meine Frage, inwieweit dies tatsächlich geschieht und inwieweit hierzu eine kontinuierliche Aufzeichnung von Zielnummern notwendig ist, wird von ihnen nicht beantwortet. Auch für Gespräche des Personalrats könne eine Sonderregelung nicht in Betracht kommen. Eine Prüfung wirtschaftlicher Verwendung von Haushaltsmitteln sei ohne Kenntnis der Zielnummern nicht durchführbar. Soweit Bedienstete private Gespräche von Dienstanschlüs-

sen führen, sei dies als „konkludente Einwilligung zur Aufzeichnung der Zielnummer" zu werten. Ich halte diese Auffassung für rechtlich nicht haltbar und sehe hierin keinen Ansatz, die unterschiedlichen Standpunkte einander anzunähern.

Daß Lösungen möglich sind, die die Interessen der Beteiligten zum Ausgleich bringen, zeigen folgende Beispiele:

— Bei der Bundesanstalt für Flugsicherung in Frankfurt wird ein Verfahren zur Telefondatenerfassung angewandt, das im wesentlichen meinen Empfehlungen aus dem Vierten Tätigkeitsbericht entspricht. Bei Auswertungen werden die vom Apparat des Personalrats aus angewählten Zielnummern nicht mitgedruckt. Den Mitarbeitern wurde in einer hausinternen Information das Verfahren der Telefonkontrolle (u. a. welche Daten wie lange wozu gespeichert werden) genau erläutert.

— Zwischen dem Vorstand der Deutschen Bundesbahn und dem Hauptpersonalrat wurde eine Dienstvereinbarung über das Verfahren der automatischen Gebührenerfassung von Postgesprächen abgeschlossen. Die Vereinbarung sieht zwar eine Erfassung der Rufnummer des angewählten Teilnehmers vor, enthält jedoch nähere Bestimmungen über die Auswertung und beschränkt diese derart, daß grundsätzlich nur ein Teil der Ziffern des Teilnehmers ausgedruckt wird.

2.4.5 Personalinformationssystem PERFIS des Bundesministers der Verteidigung

In meinem Dritten (S. 28) und Vierten Tätigkeitsbericht (S. 10 f.) habe ich über eine Prüfung des Systems PERFIS („Personalführungs- und -informationssystem Soldaten") berichtet. Als Ergebnis der damaligen Prüfung hat der Bundesminister der Verteidigung eine Vielzahl meiner Anregungen aufgegriffen und das System entsprechend dem technischen Fortschritt weiterentwickelt. Im Jahre 1982 habe ich diese neuen Maßnahmen auf ihre praktische Brauchbarkeit hin nochmals überprüfen lassen. Diese Kontrolle konzentrierte sich auf die Systemsicherheit insgesamt, und zwar mit folgenden Schwerpunkten:

— Zugriffsregelungen und Zugriffssicherungen, insbesondere bei der Datenfernverarbeitung;

— Schnittstellen zu anderen Systemen des Bundesministers der Verteidigung, die für Zwecke der Personalführung genutzt werden;

— Bundeswehrerkennungsdienst.

Nach meinem Gesamteindruck erscheint PERFIS ausreichend sicher. Meine früher geäußerte Auffassung, daß PERFIS keine lückenlose Kontrolle der tatsächlich abgewickelten Arbeitsaufträge ermögliche, ist damit hinfällig. Auch haben sich bei der Untersuchung der Schnittstellen keine Anhaltspunkte dafür ergeben, daß die Verbindungen zu anderen Informationssystemen des Bundesministers der Verteidigung aus datenschutzrechtlicher Sicht unzulässige oder problematische Datenflüsse entstehen lassen.

Gegenwärtig können das Ist an Personal und das Soll nur manuell miteinander abgeglichen werden. Es gibt im Bundesministerium der Verteidigung aber Erwägungen, in Zukunft Verfahren für einen automatischen Soll-Ist-Vergleich realisieren zu können. Für diesen Fall — in Fachkreisen wird zumeist nur bei einer derartigen technischen Möglichkeit von „wirklichen" Personalinformationssystemen gesprochen — werden sich auch Datenschutzfragen anders stellen.

Noch nicht realisiert wurde meine Anregung, die Revisionsbefugnisse für das System PERFIS, die einer besonderen Gruppe obliegen, zu erweitern. Gegenwärtig erstrecken sich diese Revisionsbefugnisse auf alle Stellen mit PERFIS-Anschlüssen; hiervon ausgenommen sind die personalbearbeitenden Referate innerhalb des Verteidigungsministeriums.

Der Bundesminister der Verteidigung ist auch meiner Anregung nicht gefolgt, den Amtshilfeverkehr des Bundeswehrerkennungsdienstes datenschutzfreundlicher zu gestalten. Der Erkennungsdienst (beim Personalstammamt in Köln) ist eine alte, historisch gewachsene Einrichtung der Bundeswehr. Das Wort geht zurück auf die Erkennungsmarke der Soldaten. Nach den entsprechenden Vorschriften ist zur Identifizierung der Soldaten u. a. auch eine „Erkennungsliste" zu führen. Der Erkennungsdienst soll als Basis für den im Verteidigungsfall einzurichtenden Bundeswehr*auskunftsdienst* dienen, zu dessen Einrichtung die Bundesrepublik auch durch das Genfer Abkommen verpflichtet ist. Genutzt wird diese Stelle gegenwärtig vor allem derart, daß an Dritte, z. B. Gläubiger, Polizei oder andere Behörden, Auskunft über Namen und Einheit der Soldaten gegeben wird. Im Monat sind dies etwa 1 000 bis 1 700 Auskunftsersuchen. Die Überprüfung hat ergeben, daß viele Anfragen sehr unspezifisch sind (z. B. Deutsche Bundesbahn „Suche eines Schwarzfahrers"), die Auskünfte selbst werden ohne besondere Prüfung durch den Erkennungsdienst erteilt. Ich hatte vorgeschlagen, diese Auskunftsersuchen besonders zu dokumentieren. Nach mehrmonatiger Erprobung hat der Bundesminister der Verteidigung davon abgesehen, ein besonderes Registrierungssystem zu schaffen, da hierfür der Aufwand zu hoch sei. Da die übermittelten Daten (Name und Einheit) nicht sehr sensibel sind, habe ich dieser Auffassung nicht widersprochen.

Beim Erkennungsdienst existiert im übrigen eine manuelle Zentralkartei der Offiziere, die sämtliche Offiziere der Bundeswehr von 1956 bis 1. Januar 1979 enthält. Meiner Anregung entsprechend wird diese für die Aufgabenerfüllung des Dienstes nicht erforderliche Kartei ausgelagert und dem Bundesarchiv übergeben werden.

2.5 Deutsche Bundespost

2.5.1 Datenschutzkontrolle und Brief-, Post- und Fernmeldegeheimnis

Die meisten personenbezogenen Daten, die die Deutsche Bundespost zu verarbeiten hat, sind — hierauf habe ich schon früher hingewiesen (4. TB S. 8) — nicht Grundlage eigener Entscheidungen, sondern Beförderungsgegenstand. Da es wohl kaum einen Bürger gibt, der nicht auch Postkunde wäre, ist verständlich, daß viele der an mich gerichteten Eingaben die Post betreffen. Ich sehe hierin nicht etwa schon ein Anzeichen für Schwächen des Datenschutzes bei der Post, wohl aber ein Indiz dafür, daß der Datenschutz hier angesichts des riesigen Volumens der verarbeiteten Daten wie auch einer rasanten technologischen Entwicklung im Bereich der elektronischen Datenübermittlung besondere Aufmerksamkeit verdient.

Die Ausgestaltung der künftigen Informationslandschaft durch Neue Medien, an deren Schaffung die Deutsche Bundespost maßgeblich beteiligt ist, bedeutet eine verstärkte Herausforderung für den Datenschutz. Die erfreulich strenge Gewährleistung des Fernmeldegeheimnisses in den herkömmlichen Bereichen des Fernmeldewesens muß auch in die neuen Übermittlungstechnologien übertragen werden. Es erscheint mir aber nicht sicher, daß es allein mit diesem Instrument gelingt, auch die künftigen Datenschutzanforderungen bewältigen zu können. Ich habe namentlich darauf hingewiesen, daß die Neuen Medien eine neue Dimension von Datensammlung und -auswertung bedeuten und die enorme Vielfalt der möglichen Kommunikationen die Kontrolle erschwert. Erneut weise ich auch auf die wiederholt und verstärkt in der Öffentlichkeit laut werdenden Besorgnisse hin, daß der Fernmeldeverkehr mit verhältnismäßig geringem Aufwand abgeleitet und abgehört werden kann (vgl. 4. TB S. 8).

Vor diesem Hintergrund ist es unbefriedigend, daß meiner Kontrollbefugnis wegen Artikel 19 Abs. 1 Satz 2 GG das Brief-, Post- und Fernmeldegeheimnis entgegengehalten werden kann. Zu den „anderen Vorschriften über den Datenschutz", deren Einhaltung bei der Deutschen Bundespost ich gemäß § 19 Abs. 1 BDSG zu kontrollieren habe, zählen zwar auch Artikel 10 GG, der das Brief-, Post- und Fernmeldegeheimnis gewährleistet, sowie dessen Ausformungen in bereichsspezifischen, das Post- und Fernmeldewesen betreffenden Gesetzen, aber das BDSG benennt das Grundrecht des Artikel 10 nicht ausdrücklich (vgl. schon 3. TB S. 30). In Einklang mit einem im Juni 1982 gefaßten Beschluß der Konferenz der Datenschutzbeauftragten der Länder und des Bundes trete ich dafür ein, gesetzlich klarzustellen, daß das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses insoweit eingeschränkt ist, als es zur Ausübung der Kontrolle bei der Deutschen Bundespost erforderlich ist.

Versuche der Post, die Kontrolle der Einhaltung „anderer Vorschriften über den Datenschutz" im Sinne von § 19 BDSG auf solche Vorschriften zu beschränken, die in Dateien gespeicherte personenbezogene Daten betreffen, gab es auch in jüngster Zeit. Schon wiederholt habe ich begründet, daß ich dieser Auffassung widersprechen muß. Erfreulicherweise gibt es aber auch Anzeichen für ein zunehmendes Verständnis dafür, daß das Brief-, Post- und Fernmeldegeheimnis und der Datenschutz nicht gegeneinander, sondern miteinander und ineinander wirken müssen, wenn es gilt, auch in Zukunft der Beeinträchtigung schutzwürdiger Belange der Postbenutzer entgegenzuwirken.

2.5.2 Aufzeichnungen über Telefongespräche

Zur Abrechnung der Fernsprechgebühren werden in der Regel lediglich die anfallenden Gebühren addiert und dem Fernsprechteilnehmer die Summe in Rechnung gestellt. Einige Ortsnetze der Deutschen Bundespost sind mit dem sogenannten elektronischen Wählsystem (EWS) ausgestattet. Auch im EWS werden im Regelfall — nicht anders als im herkömmlichen Verfahren — lediglich die Gebühren addiert. Das EWS bot aber erstmals die technische Möglichkeit, ohne allzu großen Mehraufwand über die Zahl der Gebühreneinheiten hinaus die angerufene Nummer (Zielnummer) sowie Datum und Uhrzeit des Gespräches festzuhalten. Im Rahmen eines Betriebsversuches, der seit 1978 bei einigen Fernmeldeämtern, die an das EWS angeschlossen waren, durchgeführt wurde, wurden diese Daten in einem zentralen Rechner in Neuss gespeichert und nach Ablauf einer bestimmten Frist gelöscht. Der Bundesminister für das Post- und Fernmeldewesen hat diesen Betriebsversuch beendet. Er hat damit den schon in meinem 3. Tätigkeitsbericht (S. 31) wiedergegebenen Bedenken sowie kritischen Reaktionen der Öffentlichkeit Rechnung getragen. Tatsächlich würde es sich bei der Speicherung von Zielnummern um Daten von einem hohen Sensibilitätsgrad handeln, die, wenn sie Unbefugten zur Kenntnis gelangten, in vielfältiger Weise mißbraucht werden könnten. Zwar bietet das Fernmeldegeheimnis einen starken Schutz, doch könnten Polizei und Nachrichtendienste sich dieser ergiebigen Datenquelle im Rahmen der ihnen gesetzlich zugewiesenen Befugnisse bedienen.

Beanstandet ein Teilnehmer seine Rechnung und verlangt über die Summe der Gesprächseinheiten hinaus ausführlichere Angaben, so kann im herkömmlichen Verfahren das Fernmeldeamt einen sogenannten befristeten Zählvergleich durchführen, bei dem neben der anrufenden Nummer auch die angerufene Nummer, Datum und Uhrzeit sowie die Zahl der Gesprächseinheiten während eines befristeten Zeitraums auf einem Zählvergleichsstreifen festgehalten werden. Die Einführung des EWS ändert nichts daran, daß eine Datenspeicherung zur Erstellung eines Einzelgesprächsnachweises nur auf Antrag des Kunden, d. h. mit dessen Einwilligung, vorgenommen wird. Der Bundesminister für das Post- und Fernmeldewesen folgt mit diesem Verfahren einem Beschluß des Postausschusses des Deutschen Bundestages, an dessen Zustandekommen ich beteiligt war (enthalten im Beschluß des Bundestages zu meinem 2. und 3. TB, Drucksache 9/1623 S. 4).

Die erfaßten Daten unterliegen dem Fernmeldegeheimnis; sie werden entsprechend geschützt und mit Erledigung des Erstattungsanspruches bzw. nach Abschluß des Streitfalles vernichtet. Der Antragsteller erhält dem Beschluß gemäß zunächst nur Datum, Anfangszeit und Ende des Gesprächs und gegebenenfalls die Vorwahlnummer des Angerufenen. Im Einklang mit den Empfehlungen des Postausschusses gibt die Post die Nummer des Angerufenen (Zielnummer) nur auf richterliche Anordnung heraus. Erfahrungen der Praxis haben die Frage aufkommen lassen, ob hiermit für die Herausgabe der Zielnummern nicht eine zu hohe Schwelle gesetzt ist. Insofern scheint mir weitere kritische Beobachtung der Praxis notwendig.

Eine solche Schwelle kann m. E. für den Fall nicht in Betracht kommen, daß ein Fernsprechteilnehmer — ohne den Anlaß eines Gebührenstreits — aus Gründen der Kostenkontrolle oder -aufteilung eine detaillierte Fernsprechrechnung wünscht. Sobald die technischen Voraussetzungen im EWS gegeben sind, wird diesem berechtigten Anliegen entsprochen werden können. Die technische Ausgestaltung des Fernsprechsystems wird daher zwei verschiedene Verfahrensweisen zulassen müssen: eine, nach der Gespräche nicht, und eine andere, nach der Gespräche nach Antrag registriert werden.

Besonderheiten gelten auch in Fällen der Betriebsstörung und der Belästigung. Eine Zählvergleichsschaltung kommt nicht nur als Mittel der Prüfung richtiger Gebührenerfassung, sondern auch zur Eingrenzung von Betriebsstörungen in Betracht. Der Bundesminister für das Post- und Fernmeldewesen hat erklärt, daß Zählvergleichsschaltungen zum Eingrenzen von Betriebsstörungen grundsätzlich mit dem Teilnehmer abgestimmt werden. Die vorherige Abstimmung unterbleibt nur in den seltenen Ausnahmefällen, wo der Zweck der Auswertung dies gebietet.

Nach § 12 Abs. 1 der Fernmeldeordnung ist jeder Fernsprechteilnehmer dafür verantwortlich, daß ein Mißbrauch der Teilnehmereinrichtungen durch ihn oder andere unterbleibt. Mißbrauch ist jede Benutzung, die gegen die Gesetze verstößt oder die öffentliche Sicherheit oder Ordnung gefährdet. Gestützt auf § 38 Abs. 3 der Fernmeldeordnung, ermittelt die Deutsche Bundespost auf Antrag eines Teilnehmers, der unter Angabe stichhaltiger Gründe vorbringt, belästigt zu werden, durch sogenannte Fangeinrichtung oder — soweit eine solche nicht möglich ist — mit Hilfe einer Zählvergleichseinrichtung, von welchem Anschluß der Antragsteller angerufen wird. Die Schaltung einer Zählvergleichseinrichtung bei dem vom Belästigten genannten Anschluß des vermeintlichen Belästigers erweist sich unter Umständen als das einzige Mittel, mißbräuchlicher Benutzung von Fernmeldeeinrichtungen zu begegnen. Eine Kenntnisnahme vom Gesprächsinhalt durch die Deutsche Bundespost ist auch bei diesen Maßnahmen ausgeschlossen.

Dem antragstellenden Teilnehmer wird mitgeteilt, ob und gegebenenfalls von welchem Anschluß zu welchem Zeitpunkt er angerufen wurde. Dem Zweck der Maßnahmen der Deutschen Bundespost entspricht es, daß eine vorherige Unterrichtung des vermeintlichen Belästigers vor Schaltung einer Zählvergleichseinrichtung nicht in Betracht kommen kann. Ich bin mit dem Bundesminister für das Post- und Fernmeldewesen jedoch im Gespräch darüber, ob nicht nachträglich Ergebnis und Anlaß der Schaltung einer Zählvergleichseinrichtung *beiden* Fernsprechteilnehmern mitgeteilt und der Beschwerdeführer über dieses Verfahren schon bei Antragstellung unterrichtet werden sollte.

2.5.3 Amtliches Fernsprechbuch, Fernsprechauskunftsdienst

Nichteintrag

Mit der datenschutzrechtlichen Problematik der Eintragung im Fernsprechbuch habe ich mich seit Jahren beschäftigt. Eingaben vieler Bürger, die sich durch häufige und unerwünschte Telefonate belästigt fühlten, gaben mir hierzu Anlaß. Der Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages hat meine bereits im Dritten Tätigkeitsbericht (dort S. 31 f) gegebenen Hinweise aufgegriffen und eine Änderung des § 39 Abs. 2 Satz 6 der Fernmeldeordnung initiiert. Die Vorschrift lautet nunmehr: „Ein Eintrag kann auf Antrag für eine angemessene Frist unterbleiben, wenn der Teilnehmer glaubhaft macht, daß für ihn oder eine andere Person im Falle der Eintragung eine Gefährdung oder erhebliche Belästigung eintreten kann."

Ich sehe in der Änderung einen Fortschritt. Die Tatsache, daß Beschwerden seltener werden, könnte ein Indiz dafür sein, daß die Post bei Entscheidungen über Anträge auf Nichteintragung großzügiger als bisher verfährt.

Haupteintrag/Ergänzung des Haupteintrages

Fernsprechbücher enthalten häufig nur den Namen (Familiennamen) und die Telefonnummer des Teilnehmers. Die Fernmeldeordnung (§ 39 Abs. 2) bezeichnet einen solchen Eintrag als „Haupteintrag", die Post nennt ihn in der Praxis aber meist „Kurzeintrag". Mit ständig zunehmender Zahl von Fernsprechteilnehmern wird das Auffinden einer gesuchten Telefonnummer bei namensgleichen Teilnehmern oft schwierig und ist häufig gar nicht möglich. Die Deutsche Bundespost wirkt daher darauf hin, daß dem Haupteintrag ergänzende Angaben hinzugefügt werden, um dem Anrufer das Auffinden der richtigen Rufnummer zu erleichtern.

Ich akzeptiere dieses Anliegen, kann jedoch der Post insoweit nicht folgen, als diese unter Berufung auf § 39 Abs. 2 Satz 3 der Fernmeldeordnung der Ansicht ist, eine Ergänzung notfalls auch gegen den Willen des Teilnehmers festlegen zu können. Ich vertrete demgegenüber die Auffassung, daß es von der freien Willensentscheidung des Anschlußinhabers abhängen sollte, inwieweit er durch Eintragung im Telefonbuch der Kommunikationssuche anderer entgegenkommen möchte. Ihm sollte — ge-

rade nachdem die Deutsche Bundespost ihm das Risiko der Verwechselung verdeutlicht hat — überlassen bleiben, ob er mit Beibehaltung lediglich des Haupteintrages sich diesem Risiko aussetzen oder sich hiergegen durch deutlicheren Eintrag schützen möchte.

Wiederholt geführte und im Jahre 1982 vertiefte Gespräche mit dem Bundespostministerium lassen hoffen, daß dieser Unterschied der Standpunkte sich künftig kaum noch praktisch auswirkt. Die Post hat in erfreulicher Weise verstärkte Anstrengungen unternommen, den Kunden über den Sinn der Änderung bzw. Ergänzung zu informieren. Besonders begrüße ich die Bereitschaft, der individuellen Interessenlage durch wahlweise Angabe von Vornamen, u. U. Titel oder akademischem Grad, einer Berufs- oder Branchenbezeichnung, Stadtteil, gegebenenfalls Straße ohne Hausnummer statt der vollen Anschrift stärker Rechnung zu tragen. Es bleibt zu beobachten, ob bei dieser Verfahrensweise noch Fälle übrig bleiben, in denen angemessene Lösungen nicht zu erreichen sind.

Fernsprechauskunftsdienst

Einige Anfragen von Bürgern gaben mir Anlaß, mich auch mit Fragen des Inhalts und Umfangs der fernmündlichen Auskunftserteilung durch die Deutsche Bundespost zu befassen.

Der Fernsprechauskunftsdienst verfügt über die Daten, die Inhalt des geltenden amtlichen Fernsprechbuches sind bzw. in dessen nächste Auflage übernommen werden sollen. Ist einem Antrag auf Nichteintragung stattgegeben, so besitzt der Auskunftsdienst keinerlei Angaben.

Grundlage der Tätigkeit des Fernsprechauskunftsdienstes ist § 33 Abs. 8 der Fernmeldeordnung, wonach die Deutsche Bundespost auf fernmündliche Anfragen die Rufnummer des gewünschten Anschlusses und/oder die Ortsnetzkennzahl des gewünschten Ortsnetzes bekanntgibt. Ich begrüße, daß — wie Gespräche mit dem Bundespostministerium ergeben haben — der Auskunftsdienst angewiesen ist, Fragen, die nicht auf das Herausfinden der gesuchten Rufnummer, sondern ersichtlich auf den der Rufnummer zugeordneten Namen oder die Anschrift zielen, nicht zu beantworten. Dies schließt nicht aus, daß der Auskunftsdienst — um den gesuchten Teilnehmer zu identifizieren — mit dem Auskunftsuchenden gegebenenfalls auch über die Anschrift des Teilnehmers spricht.

2.5.4 Deutsche Postreklame

Immer wieder bis in die jüngste Zeit erhalte ich Eingaben von Postkunden zur Übermittlung von Anschriften an die Deutsche Postreklame. Auf meine Anregung hin hatte seinerzeit der Bundesminister für das Post- und Fernmeldewesen den Antrag auf Fernmeldehauptanschlüsse um einen Hinweis darauf ergänzt, daß es dem Fernmeldekunden freigestellt ist, ob er der Weitergabe seiner Anschrift zu Werbezwecken an die Deutsche Postreklame zustimmt oder nicht. Die Zahl der Eingaben, in denen ich um Hilfe bei der Löschung aus den Dateien der Deutschen Postreklame gebeten wurde, ist daraufhin spürbar zurückgegangen.

Ich erinnere in diesem Zusammenhang auch an eine weitere, jedem Bürger zur Verfügung stehende Möglichkeit, sich gegen die Zusendung von Werbematerial zu schützen: durch einen Eintrag in die sogenannte „Robinson-Liste“ des Verbandes der Adressenverleger und Direktwerbeunternehmer, Neue Kräme 27, 6000 Frankfurt am Main 1. Die in diesem Verband zusammengeschlossenen Adressenverlage (einschließlich der Deutschen Postreklame), aber auch zahlreiche Versandhäuser und andere Firmen, die Werbedrucksachen verschicken, haben sich bereit erklärt, alle in diese Liste aufgenommenen Verbraucheradressen aus ihren Karteien zu entfernen und diesen Verbrauchern kein Werbematerial mehr zu schicken.

Es war wohl nur ein „Ausrutscher“, daß in der Werbeschrift „Werben per Post“, die kürzlich vom Bundesminister für das Post- und Fernmeldewesen herausgegeben wurde, der Personenkreis derer, die sich in die Robinson-Liste eintragen lassen, als „die Kontaktallergischen“ umschrieben worden ist. Das Ministerium hat zugesagt, diesen Ausdruck aus der Pathologie künftig zu vermeiden.

2.5.5 Einzelne Dienstleistungen der Post

Anschriftenänderungsdienst

In einem Schriftwechsel zu Fragen der Anschriftenprüfung nach Wohnungswechsel des Postkunden hat mir das Bundespostministerium bestätigt, daß die Behörden der Deutschen Bundespost angewiesen sind, in Fällen, in denen der Postkunde einer Anschriftenmitteilung an Absender oder Dritte schriftlich widersprochen hat, von einer Mitteilung der Anschrift abzusehen (vgl. schon 3. TB S. 32). Die dem Kunden eingeräumte Möglichkeit, der Anschriftenmitteilung jederzeit zu widersprechen, entspricht dem Prinzip, daß der Bürger in erster Linie selbst entscheiden sollte, wem er seine Anschrift überläßt, d. h. mit wem er postalisch kommunizieren will. Ich halte es aber auch für erforderlich, dem Bürger seine Dispositionsmöglichkeiten zumindest dann zu verdeutlichen, wenn er einen Nachsendeantrag stellt. In mir vorliegenden Eingaben beklagen sich Petenten darüber, daß Formulare für Nachsendungsanträge eine Aufklärung über die Entscheidungsmöglichkeit des Bürgers nicht enthalten.

Ich habe dem Bundesminister für das Post- und Fernmeldewesen daher 1982 erneut vorgeschlagen, diesem Anliegen zu entsprechen. Der Bundesminister für das Post- und Fernmeldewesen hat diesen Vorschlag jedoch mit der Begründung abgelehnt, dadurch werde die Post mit zuviel Irrläufern belastet. Die Post stellt damit ihre Kostenerwägungen über die Wünsche einer gewiß kleinen Zahl ihrer Kunden und versucht, einzelne Bürger, die gute Gründe für ihr Verhalten haben können, zur Anpassung an andere zu erziehen.

Anschriftenprüfung bei Postfächern

Um zu vermeiden, daß ihre volle Privatanschrift Dritten bekannt wird, lassen sich manche Postkunden ein Postfach einrichten. Wenn in solchen Fällen die Post die Anschrift des Postfachinhabers dem Absender oder Dritten bekanntgibt, vereitelt sie diesen Zweck.

Dies habe ich bereits früher mit dem Bundesminister für das Post- und Fernmeldewesen erörtert. Er hat daraufhin die Oberpostdirektionen angewiesen, von einer Mitteilung der Anschrift an Absender oder Dritte abzusehen, wenn der Empfänger dem schriftlich widersprochen hat. Ich halte dies für eine datenschutzrechtlich vertretbare Lösung.

Postscheckdienst

Jedes Postscheckkonto enthält eine Kontonummer und eine Kontobezeichnung. Nach § 4 Abs. 2 der Postscheckordnung muß das Postscheckkonto so bezeichnet sein, daß über den Kontoinhaber kein Zweifel besteht. Nach entsprechenden Ausführungsbestimmungen sind Vor- und Zuname sowie Orts- und Zustellangabe Bestandteile der Kontobezeichnung.

Im Einklang mit meinen Anregungen hat sich das Bundespostministerium erfreulicherweise bereiterklärt, schutzwürdigen Belagen des Kontoinhabers Rechnung zu tragen und in solchen Fällen, in denen dieser das ausdrücklich gewünscht hat, die Adresse an Auskunftsuchende nicht weiterzugeben.

2.5.6 Neue Kommunikationstechniken

Neue Dienstleistungen in der Datenkommunikation

Unter der Bezeichnung DATEX-P stellt die Deutsche Bundespost ein neues automatisches Datenvermittlungssystem vor, das sich durch hohe Wirtschaftlichkeit und Leistungsfähigkeit auszeichnet. Kennzeichnend ist hierbei, daß eine Datenverbindung zwischen zwei EDV-Anlagen nicht als Zusammenschaltung einer individuellen (körperlichen) Leitungsverbindung realisiert wird, sondern daß die zu übertragenden Nachrichten durch einen Rechner in „Pakete" zerlegt werden, die über momentan freie, in der Regel unterschiedliche, Leitungswege geführt und erst am Ende der Verbindung wieder zusammengefügt werden. Durch geeignete technisch-organisatorische Verfahren der Datensicherung muß hierbei sichergestellt werden, daß sowohl bei technischen Störungen als auch gegenüber Manipulationen Unbefugter für die Betroffenen ein ausreichender Datenschutz gewährleistet ist. Technisch erforderliche Registrierungen von Betriebsabläufen und -zuständen dürfen nur zweckgebunden verwendet werden.

Mit Teletex wird ein neues Textübertragungssystem bezeichnet, das neben größerem Komfort für den Anwender auch eine vielfach höhere Übertragungsgeschwindigkeit bietet. Neben Forderungen zur Datensicherung, die analog zu DATEX-P zu erheben sind, ist auch hier sicherzustellen, daß im zentralen Rechner keine nicht erforderlichen und deshalb unzulässigen Speicherungen vorgenommen werden.

Besondere Risiken im elektronischen Wählsystem

Bereits unter Punkt 2.5.2 habe ich auf solche Probleme hingewiesen, die sich durch das elektronische Wählsystem (EWS) zwar verschärfen, im Prinzip jedoch bereits auch bei der konventionellen Technik gegeben waren. Eine neue Gefährdung im EWS ergibt sich aus der Tatsache, daß Auf- und Abbau einer Fernsprechverbindung vom Rechner gesteuert werden. Dies ermöglicht nicht nur neue Leistungen im Fernsprechdienst, wie z. B. Anrufsperre, automatischen Weckdienst und später auch selbst aufgebaute Konferenzschaltungen, sondern schafft auch zusätzliche Risiken. So wird z. B. in der konventionellen Wähltechnik eine bestehende Fernsprechverbindung gegen versehentliches oder böswilliges Aufwählen eines Dritten durch elektromechanische Vorkehrungen „hardwaremäßig" geschützt. Sehr selten auftretende Fehler an den entsprechenden Einrichtungen gestatten von einem Teilnehmer-Anschluß aus allenfalls ein versehentliches, ungezieltes Eintreten in fremde Verbindungen, nicht jedoch ein vorsätzliches Aufschalten, gezielt auf eine bestimmte Verbindung. Letzteres ist zur Störungsprüfung nur an Leitungsverteilern und in den Vermittlungsstellen der Post möglich. Im EWS hingegen müssen solche Schutzvorkehrungen durch das Programm des Rechners geschaffen werden. Die Deutsche Bundespost wird der Sicherheit des EWS gegen unzulässigen Eintritt eines Dritten in eine Verbindung große Aufmerksamkeit widmen müssen.

Der Betrieb solcher Systeme einschließlich der Störungsbeseitigung erfordert, daß zu Wartungszwekken von einem normalen Teilnehmeranschluß aus durch Wahl entsprechender Codezahlen Zugang zum System hergestellt werden kann. Damit können z. B. Meß- und Kontrollprogramme initiiert werden. Dabei besteht auch die Möglichkeit, zu Kontrollzwecken kurzzeitig in ein bestehendes Ferngespräch einzutreten. In der Presse ist gelegentlich die Besorgnis geäußert worden, daß durch diese gegenüber herkömmlicher Technik erheblich vereinfachte Möglichkeit des Mithörens von Ferngesprächen diese Systemzugänge mißbraucht werden könnten. Es wird zu prüfen sein, ob die von der Post getroffenen Schutz- und Kontrollmaßnahmen einen wirksamen Schutz gegen Mißbrauch gewährleisten.

2.6 Medien

2.6.1 Rundfunkanstalten des Bundesrechts

Für die beiden Rundfunkanstalten des Bundesrechts, Deutsche Welle und Deutschlandfunk, gilt das Bundesdatenschutzgesetz weitgehend nicht, soweit die Anstalten personenbezogene Daten ausschließlich für eigene publizistische Zwecke verar-

beiten. Ich hatte deshalb in den Jahren 1980 und 1981 dort nur die anderen Bereiche der Datenverarbeitung überprüft und dabei seinerzeit festgestellt, daß einige Dateien nicht oder nicht richtig nach § 12 BDSG im Bundesanzeiger veröffentlicht und einige automatisch betriebene Dateien nicht zu meinem Register nach § 19 Abs. 4 BDSG gemeldet worden waren. Außerdem bestanden nicht unerhebliche Mängel bei der Organisation des Datenschutzes und bei der Datensicherung (vgl. 3. TB S. 33, 4. TB S. 10).

Im Anschluß daran bin ich deshalb im Jahre 1982 gern der Bitte des Deutschlandfunks gefolgt, bei der Verbesserung des Datenschutzes beratend mitzuwirken. Mitarbeiter meiner Dienststelle und des Deutschlandfunks haben gemeinsam ein Konzept für die Organisation des Datenschutzes beim Deutschlandfunk entwickelt. Dazu gehören z. B. Vordrucke, mit denen Dateien so beschrieben werden, daß der interne Datenschutzbeauftragte daraus erkennen kann, ob die Datenverarbeitung zulässig ist, ob die Datei veröffentlicht und ob sie zu meinem Register gemeldet werden muß. Ferner wurden die Informationsbeziehungen zwischen den einzelnen Organisationseinheiten und der EDV-Abteilung unter Einbeziehung des internen Datenschutzbeauftragten datenschutzgerecht präzisiert. Dieses Konzept zur Organisation des Datenschutzes beim Deutschlandfunk sollte ursprünglich von einem Wirtschaftsberatungsunternehmen erarbeitet werden; durch meine Beratung konnten die Kosten, die dadurch entstanden wären, eingespart werden.

Zwischen dem Deutschlandfunk und den anderen Rundfunkanstalten werden aufgrund einer Vereinbarung regelmäßig Daten über freie Mitarbeiter ausgetauscht. Immer wenn der Deutschlandfunk oder andere Rundfunkanstalten einen freien Mitarbeiter beschäftigen, der bei einer anderen Anstalt fest angestellt ist, wird diese Anstalt von der Nebentätigkeit ihres Mitarbeiters unterrichtet. Diese Datenübermittlungen sind nicht durchweg gesetzlich zugelassen. Das gilt unabhängig von der streitigen Frage, ob hier § 10 oder (über § 7 Abs. 3) § 24 BDSG einschlägig ist. In Betracht kommen nur die gesetzlichen Regelungsalternativen „für die Aufgabenerfüllung der Datenempfänger erforderlich" (§ 10 BDSG) oder „zur Wahrung berechtigter Interessen der Datenempfänger erforderlich" (§ 24 BDSG). Der Datenempfänger muß als Arbeitgeber darauf achten, das arbeitsvertragliche Vertrauensverhältnis zwischen ihm und seinen Mitarbeitern nicht zu stören. Daraus folgt die Verpflichtung, die erforderlichen Angaben zunächst beim Arbeitnehmer selbst zu erfragen und sich nur dann an Dritte zu wenden, wenn die Vermutung besteht, daß zulässige Fragen nicht korrekt beantwortet wurden. Nur unter dieser Voraussetzung ist die Datenübermittlung durch den Dritten als erforderlich gemäß § 10 bzw. § 24 BDSG anzusehen. Sollen die Daten dagegen in allen Fällen übermittelt werden, so muß dazu die Einwilligung aller Betroffenen eingeholt werden. Ich habe darauf hingewiesen, daß dies bisher nicht sichergestellt ist. Der Intendant hat mir daraufhin mitgeteilt, daß die zwischen Rundfunkanstalten und freien Mitarbeitern geschlossenen Verträge entsprechend ergänzt werden sollen.

2.6.2 Datenschutz bei Neuen Medien

Die Einführung der Neuen Medien wird seit einigen Jahren durch Pilotprojekte vorbereitet. Zu den damit entstehenden neuen Datenschutzproblemen habe ich im Dritten (S. 33 f.) und im Vierten Tätigkeitsbericht (S. 9 f.) ausführlich Stellung genommen. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich eingehend mit dem Thema und beschloß als Ergebnis ihrer Beratungen „Grundsätze für den Datenschutz bei den Neuen Medien". Diese sind als Anhang 2 zu meinem Dritten Tätigkeitsbericht (S. 66 ff.) veröffentlicht.

Die Pilotprojekte werden durch wissenschaftliche Untersuchungen begleitet, deren erste Auswertungen vor wenigen Tagen vorgelegt wurden.

Für Ende 1983 ist die Aufnahme des Wirkbetriebes für das neue Kommunikationssystem Bildschirmtext (Btx) geplant, und die Bundespost beabsichtigt, schon im Jahr 1984 Bildschirmtext für etwa 50% aller Haushalte anzubieten. Durch diese absehbare Entwicklung gewinnt das Thema zunehmende Aktualität.

Um die politischen Konsequenzen aus den technischen Möglichkeiten und ihren voraussichtlichen Weiterentwicklungen vorzubereiten, hat der Deutsche Bundestag die Enquete-Kommission „Neue Informations- und Kommunikationstechniken" eingesetzt, in deren Unterkommission „Recht" neben anderen Problemen auch Fragen des Datenschutzes diskutiert wurden. Zu diesen Beratungen habe ich durch mehrere zum Teil ausführliche Stellungnahmen beigetragen. Einige mir wichtig erscheinende Punkte daraus fasse ich nachfolgend kurz zusammen.

Solange die neuen Techniken nur dazu genutzt werden, die Zahl der bisherigen Fernseh-Programmangebote zu erhöhen, treten keine neuen Datenschutzprobleme auf. Dies ändert sich, wenn der Teilnehmer nicht nur Empfänger ist, sondern auch zum Absender von Informationen wird, etwa um eine Reaktion auf eine empfangene Nachricht abzugeben oder um seine individuellen Informationswünsche anzuzeigen, damit sie vom System teilnehmerbezogen erfüllt werden können. Diese wechselseitigen Informationsbeziehungen bestehen z. B. beim Zweiweg-Kabelfernsehen und beim Bildschirmtext. Weil die Datenschutzprobleme in solchen Systemen stets durch das Senden von Informationen vom Teilnehmer an das System entstehen, sind die aus der Erfahrung mit den Bildschirmtext-Versuchsprojekten abgeleiteten Überlegungen auch für andere Systeme repräsentativ.

Typisch für die Btx-Kommunikation ist, daß der Teilnehmer im *Dialog* mit dem System bestimmt, was geschieht, z. B. welche Angebote er wie lange auf den Bildschirm haben will. Seine Mitteilungen gegenüber dem System können vollständig registriert werden, ohne daß er sich dessen stets be-

wußt sein dürfte. Damit begegnet uns im Btx ein technisches Instrumentarium, das Persönlichkeitsprofile möglich macht. Im Dialogverkehr mit der Teilnehmer-Zentrale, bei der alle Teilnehmer-Äußerungen und Abrufe auflaufen, entstehen qualitativ und quantitativ neue Informationen, die — falls sie festgehalten würden — umfassende Persönlichkeitsbilder ermöglichten. Der Teilnehmer bekundet bei seinen Abrufen Informationswünsche und Interessen, die in ihrer Anhäufung Rückschlüsse auf seine Persönlichkeitsstruktur zuließen.

Dies wird deutlich, wenn man bedenkt, daß beispielsweise Informationen aus den Bereichen Politik, Wirtschaft, Freizeit/Hobby, Reisen, Sport und Unterhaltung, daß Waren des täglichen Bedarfs (Versandhandel) und sonstige Dienstleistungen, Weiterbildungskurse und Lesestoff, schließlich auch die Abwicklung des Geldverkehrs angeboten werden. Dabei können weit detailliertere Einzelerkenntnisse entstehen, als dies heute etwa beim Kauf oder beim Abonnieren einer Zeitung oder beim Entleihen eines Buches möglich ist, denn die Artikel werden einzeln abgerufen, und der Lesestoff wird Seite für Seite angefordert; damit kann sogar die jeweilige Lesezeit erkannt werden. Selbst Denkvorgänge werden rekonstruierbar, so etwa die Lösung von Aufgaben im Fernunterricht, der Verlauf von Computerspielen oder das Vorgehen bei der Benutzung des Suchbaums oder eines Warenkatalogs. Bedient sich der Teilnehmer dieses Mediums auch zur Erledigung seiner privaten oder geschäftlichen Korrespondenz (elektronischer Brief), so vertraut er dem System auch seine individuellen Kommunikationsbeziehungen, deren Inhalt und Partner an. Es ist anzunehmen, daß es dafür Interessenten außerhalb des systembedingten Kreises von Beteiligten gibt, z. B. Marketingforscher, Adressenverlage, Auskunfteien, die Werbewirtschaft, die Polizei, Nachrichtendienste oder das Finanzamt.

Denkbar wäre — insbesondere angesichts der erwähnten hohen Teilnehmerzahl und der bekannten Sicherungsmängel im Telefonnetz — eine *illegale* Nutzung solcher Daten, aber fast noch interessanter erschienen die *legalen* Nutzungsmöglichkeiten; sie erhielten möglicherweise eine völlig veränderte Qualität. So würde es m. E. einen Unterschied ausmachen, ob die Nachrichtendienste Briefe öffnen oder Telefongespräche abhören dürfen oder ob sie auch wahrnehmen dürfen, welche Informations- und Unterhaltungsangebote jemand über Btx oder Kabelfernsehen nutzt, wobei hier die Informationen ohne überflüssigen Ballast und leicht auswertbar zur Verfügung stünden. Es wäre wohl auch legal, aber kaum legitim, wenn all die Daten unter Marketingaspekten ausgewertet würden, die jemand über sich abgibt, wenn er über Btx nach Freizeitangeboten sucht oder bestimmte Waren bestellen will.

Die Risiken und Gefährdungen für die Persönlichkeitssphäre der Beteiligten müssen, soweit das BDSG und die Landesdatenschutzgesetze nicht zu befriedigenden Lösungen führen, durch Spezialrecht ausgeschlossen oder zumindest gemindert werden. Meine Vorstellungen hierzu habe ich gegenüber der Enquete-Kommission wie folgt nach Stichworten zusammengefaßt:

— Grunddaten

  Zur Abwicklung des Betriebes sind Grunddaten (z. B. Name, Anschrift, Telefonnummer) erforderlich. Hierfür besteht kein Regelungsbedarf, weil das BDSG die Speicherung der erforderlichen Daten erlaubt.

  Wenn trotzdem die Grunddatenspeicherung z. B. in einer Nutzungsordnung explizit geregelt werden soll, ist darauf zu achten, daß nur erforderliche Datenarten in den Katalog aufgenommen werden, also beispielsweise nicht Schulbildung, Beruf, Familienstand, Religion.

— Daten des Seitenabrufs

  Es sollte geregelt (klargestellt) bzw. durch Systemgestaltung gesichert werden, daß Einzelangaben über Art, Inhalt und Häufigkeit der vom Teilnehmer durchgeführten Informationsabrufe höchstens bis zum Ende der jeweiligen Anschaltung gespeichert und nicht übermittelt werden.

  Die Bezahlung gebührenpflichtiger Informationsabrufe muß auf der Grundlage zweier voneinander getrennter Rechtsverhältnisse erfolgen:

  a) Anbieter — Zentrale

  b) Teilnehmer — Zentrale

  Im Regelfall werden nur Summenzähler geführt; auf Wunsch des Teilnehmers oder aus anderen wichtigen Gründen können im Einzelfall genauere Aufzeichnungen erfolgen, s. auch: Wahrung der Rechte des Teilnehmers.

— Individualkommunikation

  Es sollte ein Verfahren gefunden werden, das die Nutzung der Btx-„Briefkästen" der Teilnehmer gegen deren Willen für Werbung in der Art von Postwurfsendungen oder Massendrucksachen verhindert.

  Empfangene Mitteilungen sollten unverzüglich gelöscht werden, wenn nicht der Absender oder der Empfänger eine andere Verfügung getroffen hat.

  Darüber hinaus bedarf es der Entscheidung,

  — ob das Versenden anonymer Briefe durch die Btx-Technik zugelassen werden soll

  — wie lange Mitteilungen dem Empfänger angeboten werden sollen und ob der Absender gegebenenfalls von der Löschung nicht abgerufener Mitteilungen Kenntnis erhalten soll.

— Dialog zwischen Teilnehmer und Anbieter-DVA

  Soweit über die Zentrale ein Dialog mit der Anbieter-DVA zu Bestellungen, Überweisungsaufträgen o. ä. geführt wird, ist die zur Abwicklung erforderliche Speicherung und Verarbeitung der Teilnehmerdaten zulässig; es besteht kein Regelungsbedarf.

  Eine darüber hinausgehende Verarbeitung dieser Daten (z. B. längere Speicherung als erforderlich) sowie das Speichern anderer im Rah-

men des Dialogs anfallender Daten (z. B. über die abgerufenen Informationen, die nicht zu Bestellungen führten, über die Eingabefehler des Teilnehmers oder über die Dauer seiner Denkphasen) bedarf in jedem Einzelfall der Einwilligung gemäß § 3 Satz 1 Nr. 2 BDSG.

— Wahrung der Rechte der Teilnehmer (Beweissicherung)

Es erscheint unangemessen, zur Wahrung der Rechte von Teilnehmern im Streitfall alle oder bestimmte Arten von Aktivitäten aller Teilnehmer automatisch aufzuzeichnen.

Es ist als Frage der Systemgestaltung zu entscheiden, auf welche Weise Teilnehmer (oder Anbieter als Empfänger von Mitteilungen) in die Lage versetzt werden, Nachweise oder wenigstens Anscheinsbeweise für eigene Aktivitäten oder für den Empfang von Mitteilungen u. ä. in den Fällen zu erbringen, in denen sie dies für nötig halten (auf besonderen Wunsch im Einzelfall oder generell).

— Personenbezogene Daten im Informationsangebot

Regelungsbedarf besteht, soweit das Medienprivileg des BDSG gilt, das von der Novellierung wahrscheinlich nicht substantiell betroffen wird. Zu entscheiden ist, ob, in welcher Form und für welche Zeit Gegendarstellungen zu berücksichtigen sind, z. B.

— als Anhang zur Darstellung, solange diese angeboten wird, oder

— in einer besonderen Gruppe jedes Anbieters, der das Medienprivileg in Anspruch nimmt, für eine noch zu bestimmende Frist auch nach dem Anbieten der Darstellung.

Zu entscheiden ist ferner, ob wegen der Flüchtigkeit des Informationsangebots und der sich daraus ergebenden Beweisprobleme für den Geschädigten jede angebotene Information für eine noch festzulegende Dauer gesichert werden muß.

— Einwilligung

Den besonderen Verhältnissen bei Btx und anderen Neuen Medien entsprechend sollte die Einwilligung in den Fällen, in denen personenbezogene Daten weitergehend, als ohnehin zulässig ist, verarbeitet werden sollen, nicht an die Schriftform gebunden werden. Eine präzise Aufklärung über die Bedeutung der Einwilligung, d. h. auch über die beabsichtigten Verarbeitungen, kann und muß in jedem Einzelfall bei oder unmittelbar vor der Abfrage der Entscheidung gegeben werden.

Dieser Grundsatz sollte bereichsspezifisch, also in Bestimmungen, die nur für Btx gelten, festgeschrieben werden.

— Fernmeldegeheimnis

Wenn keine besondere Rechtskonstruktion gewählt wird, unterliegen alle auftretenden Daten zumindest vorübergehend dem Fernmeldegeheimnis.

Es ist zu entscheiden, ob und in welcher spezifischen Ausprägung die Vorschriften des § 100a StPO und des Gesetzes zu Artikel 10 GG angewendet werden sollen.

Parallel zu den Überlegungen, die ich für die Beratungen der Unterkommission „Recht" der Enquete-Kommission entwickelt habe, ist von den zuständigen Stellen in den Ländern, die insoweit für sich Regelungskompetenzen in Anspruch nehmen, die datenschutzrechtliche Problematik von Btx untersucht worden. An der Vorbereitung eines inzwischen vorliegenden Entwurfs für einen Staatsvertrag über Btx habe ich mich in einer Arbeitsgruppe — unter Beschränkung auf die inhaltlichen Aussagen zum Datenschutz — beteiligt. Dabei ist es gelungen, meine wesentlichen Forderungen in dem Entwurf zu realisieren. Dazu nenne ich einige Einzelheiten:

So ist zunächst klargestellt, daß die jeweiligen Vorschriften über den Schutz personenbezogener Daten gelten, soweit nicht der Staatsvertrag selbst etwas anderes bestimmt (Artikel 9 Abs. 1 des Entwurfs). Btx-„Betreiber" (also diejenigen, die — wie vor allem die Post — zur Nutzung von Btx technische Einrichtungen für andere bereitstellen) „dürfen personenbezogene Daten über die Inanspruchnahme einzelner Angebote nur erheben und speichern, soweit und solange diese erforderlich sind, um

— den Abruf von Angeboten zu vermitteln (Verbindungsdaten),

— die Abrechnung der für die Inanspruchnahme der technischen Einrichtungen und der Angebote seitens des Teilnehmers zu erbringenden Leistungen zu ermöglichen (Abrechnungsdaten) (Artikel 9 Abs. 2).

Wichtig ist auch Artikel 9 Abs. 3 des Staatsvertrags-Entwurfs; danach soll die Speicherung der Abrechnungsdaten so gestaltet werden, „daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Teilnehmer beantragt eine andere Art und Weise der Speicherung". Diese Bestimmung wird sich freilich nur bewähren, wenn der Ausnahmefall nicht zur Regel wird. Vorgesehen ist auch eine Bestimmung, wonach die Abrechnungsdaten nur aufgrund einer besonderen Rechtsvorschrift übermittelt werden dürfen und an Anbieter nur, soweit eine Forderung auch nach Mahnung nicht beglichen wird. Ich habe die Empfehlung gemacht, der Post das volle Inkasso zu übertragen; damit würden unzählige Einzelübermittlungen an die Anbieter (Abrechnungsdaten über oft ganz geringe Beträge!) überflüssig — was auch kundenfreundlicher wäre. Man sollte ferner überlegen, ob nicht die Herausgabe von Abrechnungsdaten von einer richterlichen Anordnung abhängig gemacht werden sollte, so wie es der Postausschuß des Bundestages für die Telefon-Abrechnung in bezug auf die Nummer des angerufenen Teilnehmers gefordert hat.

Der Anbieter darf nach dem Staatsvertrags-Entwurf vom Teilnehmer personenbezogene Daten nur

erheben und speichern, „soweit dies für das Erbringen der Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses erforderlich ist". Diese Formulierung ist sehr weit, und es besteht die Gefahr, daß damit der Geltendmachung vielfältiger privater Interessen durch entsprechende Vertragsgestaltungen zu großer Spielraum eingeräumt wird. Zumindest aber sollten solche Formen der Datennutzung, die nicht durch den eigentlichen Zweck der jeweiligen Btx-Nutzung gedeckt sind, nur mit Einwilligung des Teilnehmers zulässig sein, und diese Nutzung (Leistung, Informationsangebot, Bestellung etc.) darf nicht davon abhängig sein, daß der Teilnehmer in eine über diesen Rahmen hinausgehende Datennutzung einwilligt. Der Staatsvertrags-Entwurf enthält Bestimmungen, die in diese Richtung gehen, aber noch verbesserungsbedürftig sind (z. B. eine Ausnahme für Kreditgeschäfte). Schließlich sind Löschungsgebote über das BDSG hinaus und ein Geheimhaltungsgebot vorgesehen.

Der Staatsvertrag ist bisher noch nicht abgeschlossen worden; er wird — in Landesrecht umgesetzt — auch nur begrenzte Wirkungen entfalten können. Mir ist bekanntgeworden, daß der Bundesminister für das Post- und Fernmeldewesen eine Benutzungsordnung vorbereitet, in der auch datenschutzrechtliche Bestimmungen enthalten sein sollen. Einzelheiten dazu habe ich noch nicht in Erfahrung bringen können. Nach meiner Auffassung können die nötigen Entscheidungen jedoch nicht allein von der Post durch eine Benutzungsordnung getroffen werden. Der Gesetzgeber — auch des Bundes — sollte sich einiger Fragen annehmen, die hier angesprochen worden sind. Insbesondere muß geregelt werden, ob und, wenn ja, inwieweit und unter welchen Voraussetzungen Einschränkungen des Fernmeldegeheimnisses zulässig sein sollen.

2.7 Verkehrswesen

2.7.1 Kraftfahrt-Bundesamt (KBA)

Das Kraftfahrt-Bundesamt, eine Bundesoberbehörde im Geschäftsbereich des Bundesministers für Verkehr, ist einer der größten EDV-Anwender in der Bundesverwaltung. Alle Aufgaben des Amtes, Kraftfahrzeugerfassung, Verkehrszentralregister, Statistik und Kraftfahrzeugtechnik, werden EDV-gestützt erledigt. Meine Tätigkeit erstreckte sich in den vergangenen fünf Jahren insbesondere auf die Kontrolle der EDV selbst sowie der beiden großen Bereiche personenbezogener Datenverarbeitung, nämlich Kraftfahrzeugerfassung und Verkehrszentralregister. Die Datensicherung des Amtes ist in den vergangenen Jahren wesentlich verbessert worden (s. dazu 4. TB S. 21).

Autoadressendienst

Zu Beginn meiner Amtszeit beschwerten sich viele Bürger darüber, daß ihre Anschrift an den Autoadressendienst weitergegeben worden sei. Einige Zulassungsstellen der Länder hatten zwar in ihren Zulassungsanträgen eine Einverständniserklärung aufgenommen, die erlaubte, über die Weitergabe der Anschrift an den Autoadressendienst zu entscheiden. Aufgrund der unterschiedlichen Formulierung kam es jedoch immer wieder zu falschen Interpretationen. Daraufhin hat der Bundesminister für Verkehr in einer „Verlautbarung zur Erklärung des Fahrzeughalters über die Auswertung der Daten" (VkBl Heft 20 v. 31. Oktober 1978) den Ländern empfohlen, die Einwilligung mit einer bestimmten Formulierung und unter Beachtung bestimmter Verfahrensgrundsätze einzuholen. Der vorgesehene Text stellt sicher, daß Inhalt und Umfang der Datenübermittlung klar und unmißverständlich beschrieben werden und der Betroffene sich somit auf der Grundlage präziser Informationen frei entscheiden kann. Seit der Einführung dieser „Zustimmungserklärung" ist die Anzahl nicht gewollter Datenübermittlungen stark zurückgegangen.

In letzter Zeit habe ich bei Beschwerden über nicht gewollte Anschriftenübermittlungen an den Autoadressendienst häufig festgestellt, daß hierfür weder das KBA noch eine andere Behörde verantwortlich war. Vielmehr hatten die Beschwerdeführer in den Verträgen über den Kauf eines Autos eine Klausel unterschrieben, wonach ihre Anschrift für Zwecke der Werbung und Marktforschung weitergegeben werden darf. Nachdem in den Zulassungs- und Umschreibungsanträgen nur noch 10 bis 15 % der Kfz-Halter der Weitergabe ihrer Anschrift zustimmen, scheinen die interessierten Wirtschaftskreise sich auf diesem Wege die gewünschten Daten zu beschaffen.

Erhebung von Beruf und Gewerbe

Meine datenschutzrechtlichen Bedenken gegen die Erhebung des Berufs bzw. Gewerbes eines Halters und die Art der Verschlüsselung dieser Daten habe ich in meinem Dritten Tätigkeitsbericht S. 35 und meinem Vierten Tätigkeitsbericht S. 21 ausführlich dargestellt. Eine einvernehmliche Lösung mit dem Bundesminister für Verkehr konnte noch nicht erreicht werden. Er hat jedoch mitgeteilt, daß er dabei ist, die Gliederung und Verschlüsselung der Berufs- und Gewerbeangaben unter Berücksichtigung der speziellen Erfordernisse des Bundesleistungsgesetzes und des Verkehrssicherstellungsgesetzes neu zu gestalten.

Datei der Fahrzeuge mit Versicherungskennzeichen

Zur Überwachung des Versicherungsschutzes bei Kleinkrafträdern, Fahrrädern mit Hilfsmotor und maschinell angetriebenen Krankenfahrstühlen führt das Kraftfahrt-Bundesamt einen zentralen Bestand der versicherungspflichtigen Fahrzeuge.

Bei einer Kontrolle habe ich festgestellt, daß einige der Karteikarten mehr Daten enthalten, als das KBA gemäß § 29f Abs. 1 Satz 1 StVZO zur Erfüllung seiner Aufgaben benötigt. Die darin begründete un-

zulässige Speicherung von Daten habe ich beanstandet. Das KBA hat daraufhin sichergestellt, daß bei neuen Anmeldungen nur die erforderlichen Daten erhoben und daß die unzulässig gespeicherten Daten bei Auskünften an Dritte nicht mitgeteilt werden. Im kommenden Jahr sollen auch diese Daten in das Auskunftssystem ZEVIS übernommen werden. Damit erledigt sich das Problem.

Verkehrszentralregister

Im Verkehrszentralregister (VZR) des Kraftfahrt-Bundesamtes werden rechtskräftige Entscheidungen wegen Ordnungswidrigkeiten, Entziehungen und Versagungen von Fahrerlaubnissen, Fahrverbote sowie strafrechtliche Verurteilungen im Zusammenhang mit der Teilnahme am Straßenverkehr erfaßt (§ 28 StVG). Für welche Zwecke und durch welche Stellen diese Meldungen verwertet werden dürfen, ergibt sich abschließend aus § 30 StVG. Zum Zwecke der Erfassung und des Bereithaltens für Auskünfte werden die eingehenden Meldungen durch das KBA in eine Hängeregistratur eingestellt und nach Registernummern (Aktenzeichen) geordnet. Zum Auffinden dieser Meldungen wurde eine automatisierte Datei mit Angaben zur Identifizierung der Person, dem Tilgungsdatum der Eintragungen und Angaben über Entziehungen und Versagungen von Fahrerlaubnissen, über Fahrverbote und über Verzichte auf Fahrerlaubnisse eingerichtet. Damit wird es möglich, in der Registratur einen Vorgang zu finden, auch wenn nur der Name, also nicht die Registernummer bekannt ist. Da diese Datei auch Bestandteil des Auskunftssystem ZEVIS ist, kann künftig auch on-line abgefragt werden, ob Eintragungen über eine Person im Verkehrszentralregister vorliegen (einschließlich der Tatsache des Fahrverbots, der Entziehung/Versagung der Fahrerlaubnis oder des Verzichts auf dieselbe).

Datenschutzrechtliche Probleme habe ich sowohl im Bereich der technisch-organisatorischen Maßnahmen als auch in der materiell-rechtlichen Ausgestaltung gefunden.

Die Probleme lagen z. B. in der Behandlung unberechtigter Anfragen, der Behandlung von Sammelsendungen, der Behandlung nicht registerfähiger Angaben auf den Meldungen und in dem Umfang der Datenübermittlung durch das KBA an anfragende Stellen im Auskunftsverfahren (siehe 2. TB S. 39f.). Insbesondere die letzte Frage hat in der Diskussion zwischen dem Bundesminister für Verkehr, dem Kraftfahrt-Bundesamt und mir einen breiten Raum eingenommen. Ich stehe auf dem Standpunkt, daß der Umfang der Auskunft sich nach dem Inhalt des Auskunftsersuchens richten muß. So genügt z. B. bei der Auskunft im Rahmen der Ausstellung eines Ersatzführerscheins die Mitteilung von Tatbeständen, die sich auf ein Fahrverbot oder die Entziehung/Versagung der Fahrerlaubnis erstrecken. Der Bundesminister für Verkehr und das KBA beharren jedoch weiterhin auf ihrem Standpunkt, daß die Regelung des § 30 StVG es rechtfertige, bei jeder Anfrage durch Gerichte und Behörden Ablichtungen aller Eintragungen zu übersenden. Zwar regelt § 30 Abs. 2 Satz 1 StVG die Frage, wie die Auskunft zu erteilen ist, so, „daß die anfragende Stelle die Akten über die der Eintragung zugrundeliegenden Entscheidung beiziehen kann". Damit hat der Gesetzgeber aber nicht entschieden, daß in jedem Falle eine Vollauskunft durch das Amt zu erteilen ist. M. E. müßte — wenn nicht § 10 BDSG direkt angewendet wird — zumindest von den Grundsätzen des § 10 BDSG ausgegangen werden, die auch allgemeinen verwaltungsrechtlichen Grundsätzen entsprechen. Entscheidend ist danach die Erforderlichkeit der einzelnen Angaben für den im Einzelfall verfolgten Zweck. Abschließend ist diese Frage noch nicht entschieden. Eine Regelung war zwar in dem Entwurf eines Verkehrszentralregistergesetzes vorgesehen. Dieses Gesetz konnte in der 8. Legislaturperiode aber nicht mehr verabschiedet werden (s. unten Nr. 2.7.3).

Bei Entziehungen oder Versagungen einer Fahrerlaubnis sieht der Vordruck, mit dem diese Entscheidung dem Kraftfahrt-Bundesamt mitgeteilt wird, auch die Mitteilung der Entscheidungsgründe anhand eines Kennzifferkataloges verschlüsselt vor. Diese Übermittlung ist, obwohl ich hierauf bereits in meinem Dritten Tätigkeitsbericht (S. 35) hingewiesen habe, rechtlich noch immer nicht abgesichert. § 13 Abs. 1 StVZO bestimmt lediglich, daß die Tatsache der Entziehung oder Versagung einer Fahrerlaubnis im Verkehrszentralregister eingetragen wird. Die Mitteilungsvorschrift des § 13b StVZO schreibt ebenfalls nur die Mitteilung von Entscheidungen vor. Lediglich der nach § 13d StVZO vorgeschriebene Vordruck A Nr. 5701 geht darüber hinaus und sieht die Angabe der Entscheidungsgründe vor. Der Bundesminister für Verkehr hat zur Erforderlichkeit der Übermittlung der Entscheidungsgründe ausgeführt, das KBA benötige diese Hinweise, um die Tilgungsfristen für die Eintragung bestimmen zu können. Dieser Auffassung kann ich mich nicht anschließen, da die Tilgungsvorschriften des § 29 StVG i. V. m. § 13a StVZO auf die Rechtsgrundlagen der Entscheidungen, nicht aber auf die (konkreten) Entscheidungsgründe abstellen. Der Bundesminister für Verkehr hat dem entgegengehalten, daß die Darstellung der Entscheidungsgründe aus folgenden Gründen erforderlich sei:

- Die Entziehung bzw. Versagung der Fahrerlaubnis stelle einen derart schwerwiegenden Eingriff in die Rechte und das Leben des Betroffenen dar, daß eine möglichst genaue statistische Darstellung der Gründe erforderlich sei, um wirksame und kontrollierbare Hilfsmaßnahmen für den betroffenen Personenkreis (z. B. Nachschulungskurse u. ä.) zu ermöglichen;
- diese Daten könnten nur vom Kraftfahrt-Bundesamt ohne allzu großen Verwaltungsaufwand zur Vorbereitung von Rechts- und allgemeinen Verwaltungsvorschriften auf dem Gebiet des Straßenverkehrs bereitgestellt werden;
- die Übermittlung der fraglichen Daten diene den auskunftsberechtigten Stellen zur schnelleren

Erfüllung ihrer rechtmäßigen Aufgaben. Der Katalog der Entscheidungsgründe sei mit den Ländern abgestimmt.

Aufgrund dieser Darstellung stelle ich meine Bedenken vorerst zurück. Ich halte jedoch daran fest, daß diese Übermittlungen im Rahmen einer umfassenden rechtlichen Regelung des Verkehrszentralregisters eine eindeutige Rechtsgrundlage erhalten müssen.

Tilgungsreife Vorgänge, d. h. solche Vorgänge, die aufgrund der Tilgungsbestimmungen des § 13a StVZO aus dem Register entfernt werden müssen, weil sie nicht mehr verwertet werden dürfen, werden nicht sofort nach Eintritt der Tilgungsreife, sondern erst dann entfernt, wenn der Vorgang im Rahmen einer erneuten Registrierung oder einer Auskunft gezogen wird (s. 4. TB S. 21). Ich habe mich zwar vergewissern können, daß eine unbefugte Verwertung ausgeschlossen ist, weil vor jeder Auskunftserteilung geprüft wird, ob die in der Akte enthaltenen Eintragungen noch weitergegeben werden dürfen. Gleichwohl führt dieses Verfahren dazu, daß im Verkehrszentralregister Eintragungen bestehen, die wegen Tilgungsreife nicht mehr darin enthalten sein dürfen. Gemäß § 29 Abs. 1 StVG ist nach Ablauf der in § 13a StVZO festgelegten Frist die Eintragung im Verkehrszentralregister zu tilgen. § 13a Abs. 8 StVZO führt aus, daß tilgungsreife Eintragungen zu entfernen oder unkenntlich zu machen sind. Näheres zum Zeitpunkt dieser Entfernung/Unkenntlichmachung ist nicht geregelt, daher ist die Tilgung unverzüglich durchzuführen. Ich habe daher die verspätete Tilgung beanstandet. Der Bundesminister für Verkehr hat daraufhin erklärt, daß eine solche Verfahrensweise zu einem Mehraufwand von acht Arbeitskräften führen würde, der vom derzeitigen Personalbestand des Amtes nicht abgedeckt werden könne. Ferner müßten zu der automatisierten Datei erhebliche Änderungen programmiert werden. Nach Auffassung des BMV ist die derzeitige Verfahrensweise auch mit den gesetzlichen Bestimmungen vereinbar, weil sichergestellt sei, daß über Eintragungen nach Ablauf der Tilgungsfrist keine Mitteilungen mehr erfolgen. Für den Betroffenen ergäben sich daher keine Nachteile.

Auch unter Berücksichtigung dieser Ausführungen bleiben meine Bedenken weiterhin bestehen, da die Registrierung tilgungsreifer Vorgänge eine unzulässige Speicherung gemäß § 9 Abs. 1 BDSG ist. Der Betroffene hat gemäß § 13a Abs. 8 StVZO i. V. m. § 14 Abs. 3 Satz 2 BDSG einen durchsetzbaren Löschungsanspruch. Zwar entstehen ihm bei der jetzigen Verfahrensweise des Amtes keine unmittelbaren Nachteile, doch führt sie zum Teil zu erheblichen Überliegefristen einzelner Eintragungen. Eine solche Verkürzung der Rechtsposition des Betroffenen halte ich nur mit Zustimmung des Gesetzgebers für vertretbar. Ich werde mich bemühen, zusammen mit dem BMV und dem KBA im nächsten Jahr eine Lösung zu finden, die die bestehenden gesetzlichen Bestimmungen erfüllt, ohne zu einem erheblichen Mehraufwand zu führen.

Neben den allgemeinen Fahrerlaubnissen der Straßenverkehrsbehörden erteilen einige Verwaltungen (Bundeswehr, Deutsche Bundesbahn, Deutsche Bundespost, Bundesgrenzschutz, Polizei) Sonderfahrerlaubnisse (§ 14 StVZO). Bei Beendigung des Dienstverhältnisses oder der Verwendung als Kraftfahrzeugführer ist die Sonderfahrerlaubnis gemäß § 14 Abs. 2 einzuziehen. Da diese Sonderfahrerlaubnisinhaber nach Ausscheiden aus dem öffentlichen Dienst aber gemäß § 14 Abs. 3 StVZO auf Antrag eine allgemeine Fahrerlaubnis erhalten können und die Führerscheinstelle in diesem Falle prüfen muß, ob nicht Tatsachen vorliegen, die den Bewerber als ungeeignet zum Führen von Kraftfahrzeugen erscheinen lassen, werden Entscheidungen der Verwaltungsbehörden und der Gerichte über Verkehrsverstöße solcher Sonderfahrerlaubnisinhaber gemäß § 13b Abs. 1 StVZO ebenfalls im Verkehrszentralregister eingetragen.

Datenschutzrechtlich problematisch bei der Mitteilung von Entscheidungen über die Entziehung von Sonderfahrerlaubnissen ist, daß eine solche Entziehung nicht nur — wie im allgemeinen Straßenverkehrsrecht — mit mangelnder körperlicher oder geistiger Eignung, sondern auch mit charakterlichen Mängeln aufgrund von dienstlichen Verfehlungen begründet werden kann. Hier können Sonderfahrerlaubnisse aufgrund dienstlicher Verfehlung entzogen werden, die keinen Verkehrsbezug haben. Diese Tatsache wird dann gemäß § 13b Abs. 1 Nr. 1 StVZO dem KBA und auch den örtlichen Straßenverkehrsämtern mit dem Entscheidungsgrund „sonstige charakterliche Fehler oder Schwächen" mitgeteilt (s. auch 4. TB S. 35).

Bei den Verhandlungen mit den Bundesministern der Verteidigung und für Verkehr bestätigte sich, daß die Entziehung der Sonderfahrerlaubnis im Verteidigungsbereich als Disziplinierungsinstrument eingesetzt wird. Der Bundesminister der Verteidigung entzieht die Sonderfahrerlaubnis auch aus Gründen, aus denen eine zivile Fahrerlaubnis nicht entzogen werden könnte.

Das Entscheidungsverfahren des Bundesministers der Verteidigung ist von mir inhaltlich nicht zu beurteilen. Mißlich ist aber zweierlei. Zum einen erhalten die zivilen Führerscheinstellen Mitteilungen auch in Fällen, in denen der zugrundeliegende Vorgang für ihre Entscheidung gar nicht berücksichtigt werden darf. Zum anderen stehen Übermittlungen im Widerspruch zu den Grundsätzen des Dienstrechts, da es sich der Sache nach um Mitteilungen über Disziplinarvorgänge handelt, ohne daß dafür eine Rechtfertigung besteht.

Die Verhandlungen werden fortgesetzt.

2.7.2 ZEVIS

Das Kraftfahrt-Bundesamt ist seit Mitte der siebziger Jahre damit befaßt, die Führung der zentralen Kraftfahrzeugbestände und des Verkehrszentralregisters auf der Basis eines Datenbankkonzepts neu zu organisieren. Das unter Beteiligung des Bundeskriminalamtes entwickelte Konzept „Zentrales Ver-

kehrsinformationssystem — ZEVIS" ist darauf gerichtet, alle Daten des zentral geführten Kraftfahrzeugbestandes und des Bestandes der Fahrzeuge mit Versicherungskennzeichen, die Personalien der im Verkehrszentralregister (VZR) Eingetragenen und die Angaben über entzogene oder versagte bzw. zurückgegebene Fahrerlaubnisse aufzunehmen. Der Zugriff durch die Benutzer soll im Online-Verkehr erfolgen. Durch die Einsparung manueller Arbeitsgänge verspricht man sich wirtschaftliche Vorteile. Darüber hinaus soll das Auskunftsverfahren wesentlich beschleunigt werden.

Der gegenwärtige Ausbaustand und die weiteren Planungen stellen sich wie folgt dar. Aus dem VZR sind die Grunddaten (Namen, Anschrift, Geburtsdatum ...) aller Betroffenen entnommen sowie Angaben über entzogene, versagte oder freiwillig zurückgegebene Fahrerlaubnisse (der eigentliche Inhalt der von Behörden und Gerichten dem VZR gemachten Meldungen wird weiterhin manuell geführt). Die Kraftfahrzeugdaten der Länder Baden-Württemberg, Schleswig-Holstein und Bayern sind vollständig in die Datenbank übernommen. Im Frühjahr 1983 sollen die Daten aller Fahrzeuge mit Versicherungskennzeichen, im Sommer 1984 schließlich die aller im Bundesgebiet mit amtlichen Kennzeichen zugelassenen Fahrzeuge in der Datenbank enthalten sein. Die Software zum Aufbau und zur Pflege der Datenbestände und für den Auskunftsbetrieb ist weitgehend fertiggestellt.

Mitte 1982 waren 87 Datenstationen mit Berechtigung zur Fernabfrage installiert, davon 77 bei Polizeidienststellen des Landes Baden-Württemberg. Bei den Datenstationen der Polizei handelt es sich um die üblichen INPOL-Terminals. Sie sind über das digitale Sondernetz der Polizei DISPOL an ZEVIS angeschlossen. Anfragen der Polizei machen bereits einen erheblichen Teil des Anfrageaufkommens an ZEVIS aus.

Der Bundesminister für Verkehr und das Kraftfahrt-Bundesamt vermeiden es gleichwohl, den Eindruck entstehen zu lassen, daß ZEVIS bereits offiziell in Dienst genommen wurde, sondern sprechen immer noch zurückhaltend von „Pilot-Anwendungen".

Der Übergang zum Dauerbetrieb wäre zur Zeit auch nicht zulässig, weil die formelle Rechtsgrundlage dafür fehlt. Die bereichsspezifische Rechtsgrundlage für Auskünfte über Kfz-Halter, § 26 Abs. 5 StVZO, richtet sich nur an die örtlichen Zulassungsstellen und gestattet nur Einzelauskünfte, und der Rückgriff auf § 10 BDSG rechtfertigt nicht den Online-Anschluß, weil die damit nach § 2 Abs. 2 Nr. 2 BDSG verbundene „Übermittlung" des gesamten Datenbestandes nicht erforderlich ist (s. unten Nr. 6.6). Das geplante Fahrzeugregistergesetz und die gesetzliche Neuregelung des Verkehrszentralregisters (s. unten Nr. 2.7.3) sollen die Rechtsgrundlagen schaffen.

ZEVIS wird erhebliche Veränderungen des Informationsaustausches und der Informationsauswertung bewirken oder doch technisch ermöglichen. Im wesentlichen hat ZEVIS die Funktion, Arbeitsabläufe und Informationsprozesse, die bisher manuell bewirkt wurden, durch Automatisierung zu beschleunigen. Die Aktualität der Registereintragungen soll steigen und die Fehlerquote sinken. Diese Automationsvorteile kommen den Benutzern des Systems, vor allen Dingen also der Polizei zugute. Die praktische Erleichterung und die qualitative Verbesserung können dazu führen, daß die Informationsnachfrage und das Übermittlungsvolumen wesentlich ansteigen. Aus der Sicht des Datenschutzes ist dagegen nichts einzuwenden, solange dies sachlich gerechtfertigt und durch ausreichende Sicherheitsvorkehrungen und Kontrollmaßnahmen ein unbefugter Gebrauch mit hinreichender Sicherheit ausgeschlossen ist. Deshalb muß durch ausreichende Datensicherungsmaßnahmen sichergestellt werden, daß ein unbefugter Gebrauch soweit wie technisch möglich verhindert wird; darüber hinaus muß der Datenverkehr protokolliert und müssen die Protokolle gezielt und stichprobenweise darauf ausgewertet werden, ob Anhaltspunkte für unbefugte Datenabrufe erkennbar sind. Wie auch bei anderen Informationssystemen muß das Sicherheitssystem parallel zur Entwicklung ausgebaut und im praktischen Betrieb getestet werden. Ich beabsichtige gemeinsam mit den Landesbeauftragten für den Datenschutz die Sicherheit des Systems ZEVIS zu überprüfen.

Bisher wird in den meisten Anfragen an das KBA zu einer bekannten Kfz-Nummer (oder Teilen davon) der unbekannte Halter gesucht. Nur in relativ wenigen Fällen (ca. 1 600 von insgesamt ca. 1 Mio. je Monat) wird zu einer Person die Anschrift oder das Kfz-Kennzeichen erfragt; diese Anfrageart bereitet dem KBA eine gewisse Mühe. Das System ZEVIS ermöglicht es künftig, ohne besonderen Aufwand unter dem Namen einer Person nach ihrer aktuellen Anschrift oder den auf sie zugelassenen Fahrzeugen zu fragen (sogenannte P-Anfrage).

Mit der — bisher noch nicht realisierten, aber geplanten — Bereitstellung dieser P-Anfrage im Rahmen des Online-Verkehrs wird technisch die Möglichkeit eröffnet, den Halterbestand mit seinen rund 30 Mio. betroffenen Bürgern wie ein Bundes-Adreßregister zu verwenden. Ein solches Adreßregister ist im Zusammenhang mit dem Personalausweisgesetz vom Deutschen Bundestag ausdrücklich abgelehnt worden. Bei der Vorbereitung des Melderechtsrahmengesetzes stand die Einrichtung von Landesadreßregistern zur Diskussion; sie wurde nicht in den Regierungsentwurf übernommen. Es wäre nicht hinnehmbar, wenn im Projekt ZEVIS allein durch die Verwaltung nun doch ein vergleichbares Register geschaffen würde. Aber auch der Gesetzgeber müßte prüfen, ob der zu Zwecken der Verkehrsverwaltung begründete Datenbestand wirklich für andere Verwaltungszwecke freigegeben werden soll und wenn ja, für welche. Selbstverständlich kann die Fragestellung der Polizei an das KBA: „Wo wohnt Herr X und welche Fahrzeuge stehen ihm zur Verfügung?" im Einzelfall für Maßnahmen der Strafverfolgung oder Gefahrenabwehr erforderlich und deshalb zulässig sein. Wird diese Frageart aber im Online-Verkehr zugelassen, so besteht die Gefahr, daß durch die technische Erleich-

terung diese Abfrageart so attraktiv wird und für so viele Zwecke genutzt wird, daß ZEVIS unter der Hand, ohne bewußte Umgehungsabsicht, die Funktion eines zentralen Adreßregisters erhält. Überdies wäre die Kontrolle, ob das System nur zu den dann zugelassenen Zwecken benutzt wird, wegen der enormen Menge der regelmäßig erteilten Auskünfte und der beschränkten Prüfkapazität äußerst schwierig.

Ich habe die Bundesminister des Innern und für Verkehr um Auskunft gebeten, wie viele vom Namen der Betroffenen ausgehende Anfragen in der Vergangenheit gestellt wurden und ob bzw. aus welchen Gründen dabei eine besondere Eilbedürftigkeit bestand. Der Bundesminister für Verkehr hat mir daraufhin einen Bericht des Kraftfahrt-Bundesamtes vom 30. Juli 1982 übersandt, aus dem sich die oben erwähnte Zahl von monatlich ca. 1 600 Anfragen der genannten Art ergibt. Zur Eilbedürftigkeit konnten keine ausreichenden Angaben gemacht werden. Diese Informationen reichen nicht aus, um die Notwendigkeit der P-Anfrage für die Polizeidienststellen zu begründen; insbesondere fehlen bisher Beispiele dafür, aus welchen Gründen unter dem Namen angefragt werden muß. Infolgedessen ist auch eine Abwägung des polizeilichen Interesses mit den dargestellten Gefahren der Zweckentfremdung und Unkontrollierbarkeit kaum möglich. Es können auch keine Maßnahmen empfohlen werden, die vielleicht verhindern könnten, daß mit der P-Anfrage ZEVIS wie ein zentrales Adreßregister genutzt wird.

Wegen der großen Bedeutung dieses Auskunftssystems und des fortgeschrittenen Stadiums seiner Realisierung halte ich eine baldige Entscheidung des Gesetzgebers für geboten. Andernfalls müßte der „Testbetrieb“ eingestellt werden. Die P-Anfrage im Online-Verkehr sollte aus den Planungen gestrichen werden.

2.7.3 Gesetzesinitiativen auf dem Gebiet des Verkehrswesens

Vorentwurf eines Fahrzeugregistergesetzes

Auf dem Gebiet der Straßenverkehrszulassung bestehen verschiedene rechtliche Regelungsdefizite. Sie sind u. a. auch durch die Datenschutzbeauftragten des Bundes und der Länder aufgezeigt worden. Der Bundesminister für Verkehr hat deshalb den Entwurf eines Fahrzeugregistergesetzes vorbereitet. An den Beratungen des Vorentwurfes hat mich der Bundesminister für Verkehr beteiligt; sie sind noch nicht abgeschlossen. In einer Referentenbesprechung haben sich die Länder dafür ausgesprochen, die notwendigen Regelungen nicht in einem gesonderten Gesetz zu treffen, sondern durch Ergänzungen des Straßenverkehrsgesetzes und der Straßenverkehrszulassungsordnung.

Ziel des Entwurfs ist es, die in die Fahrzeugregister der Zulassungsstellen (örtliche Fahrzeugregister) sowie des Kraftfahrt-Bundesamtes (zentrales Fahrzeugregister) aufzunehmenden Daten festzulegen und ihre Verwertung detailliert zu regeln.

Der Gesetzentwurf sieht aber ausdrücklich auch vor, daß andere Behörden (Gerichte, Staatsanwaltschaften, Polizei, Bundeskriminalamt, Landeskriminalämter) in dem Register Suchvermerke und Steckbriefnachrichten niederlegen können. Dies dient außer Maßnahmen im Zusammenhang mit dem Straßenverkehr (z. B. Einziehung der Fahrerlaubnis) auch der Strafverfolgung, der Strafvollstreckung, der Verfolgung von Ordnungswidrigkeiten und der polizeilichen Gefahrenabwehr, und auch für Zwecke des Verfassungsschutzes, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes können Suchvermerke niedergelegt werden. Durch die Eröffnung dieser Möglichkeiten geht die Bedeutung des Registers weit über die ursprüngliche Aufgabenstellung, nämlich die Registrierung der zum Verkehr zugelassenen Fahrzeuge und die statistische und verkehrsbezogene Auswertung dieser Daten, hinaus. Ich habe erhebliche Zweifel, ob diese Erweiterung erforderlich und zulässig ist. Durch sie wird das Zulassungswesen zu einem Hilfsmittel der Vollzugspolizei und der Nachrichtendienste. Dies bedarf jedenfalls der parlamentarischen Entscheidung.

Der Entwurf enthält für die örtlichen wie auch für das zentrale Fahrzeugregister detaillierte Regelungen der Datenübermittlung, die die Rechtsklarheit verbessern. Der Aufzählung folgt jedoch jeweils eine Generalklausel, nach der für *weitere* Fälle das Erforderlichkeitsprinzip gelten soll. Ich halte nur eine Lösung für akzeptabel, bei der Auffangtatbestände vermieden oder aber an deutlich verschärfte Voraussetzungen gebunden werden. Dies ist um so wichtiger, als der Vorentwurf den Online-Zugriff sowohl auf das örtliche als auch das zentrale Fahrzeugregister für zulässig erklärt.

Entwurf eines Gesetzes über das Verkehrszentralregister

Seit 1979 laufen Bemühungen, das Verkehrszentralregister grundlegend zu reformieren. Meine datenschutzrechtlichen Vorstellungen (siehe hierzu auch oben Nr. 2.7.1) habe ich dem Bundesminister für Verkehr vorgetragen. Der Gesetzentwurf (BT-Drucksache 8/3900) berücksichtigte sie zum Teil. Zur parlamentarischen Beratung ist es nicht mehr gekommen. Der Deutsche Bundestag hat nunmehr den Initiativentwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes verabschiedet (BGBl I S. 2090), der die Eintragungsgrenze bei rechtskräftigen Entscheidungen wegen einer Ordnungswidrigkeit auf DM 80,— anhebt. Gleichzeitig hat er die Bundesregierung aufgefordert, ein umfassendes Verkehrssicherheitskonzept vorzulegen und dabei auch das Verkehrszentralregister zu reformieren. Auf die Berücksichtigung der datenschutzrechtlichen Anliegen werde ich achten.

Dritte Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften

Der Bundesminister für Verkehr hat mich an den Beratungen eines Referentenentwurfs einer Dritten Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften beteiligt, der im wesentlichen die zwingend zu übernehmenden Regelungen der Ersten Richtlinie des Rates der Europäischen Gemeinschaft zur Einführung eines EG-Führerscheins (Amtsblatt der Europäischen Gemeinschaft L/375 vom 31. Dezember 1980) sowie das Muster des Führerscheins in das deutsche Straßenverkehrsrecht umsetzen bzw. einführen soll. Datenschutzrechtlich relevant war insbesondere die Vorschrift des § 9c des Entwurfs, die vorschreibt, daß Bewerber für eine Fahrerlaubnis der Klasse 2 sich einer ärztlichen Untersuchung über ihren Gesundheitszustand zu unterziehen haben und darüber eine Bescheinigung nach vorgeschriebenem Muster der Fahrerlaubnisbehörde vorzulegen haben. Aus dieser Bescheinigung soll hervorgehen, ob Beeinträchtigungen des körperlichen oder geistigen Leistungsvermögens vorliegen, die Bedenken gegen die Eignung des Bewerbers zum Führen von Kraftfahrzeugen begründen oder Anlaß für weitergehende Untersuchungen vor Erteilung der Fahrerlaubnis geben. Der Inhalt der vorgesehenen Bescheinigung geht jedoch weit über die Feststellung, ob derartige Bedenken bestehen, hinaus und fordert vom untersuchenden Arzt die Bekanntgabe konkreter Diagnosen und Erläuterungen zu einzelnen Teilbereichen, wie Art der Herz-/Kreislaufstörungen, Art der Erkrankungen der Nieren usw. Die Kenntnis dieser Daten halte ich für die Entscheidung der örtlich zuständigen Behörde nicht für erforderlich. Nach meinem Dafürhalten muß die Angabe des untersuchenden Arztes ausreichen, ob eine Beeinträchtigung des körperlichen oder geistigen Leistungsvermögens, die eine Versagung der Fahrerlaubnis begründen kann, vorliegt oder nicht; welche Beeinträchtigungen dies sind und in welchem Umfange diese bestehen, ist nicht entscheidungsrelevant. Der Bundesminister für Verkehr hat den Vordruck daraufhin in zwei Teile gegliedert. Der Teil I dient dem Arzt als Unterlage zur Vornahme der einzelnen Untersuchungen und verbleibt bei ihm, der Teil II des Vordruckes ist die eigentliche Bescheinigung zur Vorlage bei der Verwaltungsbehörde. Aus dieser Bescheinigung ergibt sich, ob der untersuchende Arzt den Antragsteller für geeignet oder weitergehende Untersuchungen für erforderlich hält. Diagnosedaten werden nicht übermittelt. Den Anforderungen des Datenschutzes ist damit genügt.

2.7.4 Bundesanstalt für Straßenwesen

Die Bundesanstalt ist eine technisch-wissenschaftliche Einrichtung des Bundes und bearbeitet die Probleme, die sich aus den vielfältigen Beziehungen zwischen Mensch, Fahrzeug, Straße, Umwelt und Gesellschaft ergeben. 1965 erhielt die Bundesanstalt den Auftrag, über den eigentlichen Straßenbau hinaus auch die Erhöhung der Leistungsfähigkeit der Straßen und die Sicherheit des Verkehrs zu untersuchen, und 1970 wurde sie aufgrund eines Beschlusses des Deutschen Bundestages zudem als zentrale Stelle für die Unfallforschung bestimmt. Diese Aufgabenstellung bringt es mit sich, daß die Bundesanstalt selbst personenbezogene Daten verarbeitet oder im Rahmen der Vergabe von Forschungsaufträgen verarbeiten läßt. Ein Schwerpunkt meiner Prüfung erstreckte sich daher auf die Bereiche der Eigen- und Fremdforschung.

Bei einer in diesem Jahr durchgeführten Kontrolle zeigte sich, daß Datenerhebung und -verarbeitung für die Eigenforschung von einem ausgeprägten Datenschutzbewußtsein bestimmt sind. Die BASt erhebt die im Rahmen von Forschungsvorhaben benötigten Daten möglichst ohne Personenbezug; dort, wo ein Personenbezug z. B. für die Verknüpfung von Datenbeständen unvermeidlich ist, wird dieser Personenbezug zum frühestmöglichen Zeitpunkt gelöscht. Datenschutzrechtliche Verbesserungsmöglichkeiten gab es bei einigen Forschungsprojekten: So habe ich empfohlen, bei einem Gemeinschaftsprojekt mit einem Automobilclub, bei dem es um die Erforschung des Geschwindigkeitsverhaltens von Autobahnbenutzern geht, die Zweckbindung der im Rahmen dieses Vorhabens erhobenen Daten in die vertraglichen Abmachungen zwischen den beiden Forschungsstellen aufzunehmen. Das bedeutet z. B. auch ein Verbot der Mitgliederwerbung mit diesen Daten.

Bei dem Forschungsprojekt „Unfälle beim Transport gefährlicher Güter" erhält die BASt über den BMV Unfallanzeigen über solche Unfälle zugesandt. Für die Forschungstätigkeit der Bundesansalt ist ein Personenbezug nicht erforderlich. Ich mußte feststellen, daß nicht in jedem Falle vorhandene identifizierende Angaben geschwärzt waren. Die BASt wird dies künftig beim Eingang der Meldungen sicherstellen.

Die Weiterleitung der polizeilichen Unfallanzeigen über den Bundesminister für Verkehr ist gerechtfertigt, da dieser die Unfallanzeigen selbst für Zwecke der Feststellung der Effizienz der Gefahrgutvorschriften auswertet, um den gesetzlichen Auftrag — Schutz der Allgemeinheit vor Schäden durch Gefahrgut — zu erfüllen (§ 3 des Gesetzes über die Beförderung gefährlicher Güter vom 6. August 1975 — BGBl. I S. 2121).

Der überwiegende Teil der Forschungsprojekte der Bundesanstalt wird durch fremde Forschungseinrichtungen abgewickelt. Die BASt trägt in diesen Fällen als Auftraggeber eine Mitverantwortung für die rechtmäßige und ordnungsgemäße Abwicklung der Forschungsvorhaben. Unter Hinweis auf den öffentlichen Auftraggeber und gegebenenfalls unter Vorlage entsprechender Empfehlungsschreiben wird der Datenzugang bei speichernden Stellen und Betroffenen erleichtert. Die Bundesanstalt muß deshalb in besonderem Maße darauf bedacht sein, daß die Forschungstätigkeit in allen Phasen der Datenverarbeitung datenschutzgerecht abläuft. Sie fordert schon jetzt in zusätzlichen Bedingungen vom Forschungsnehmer besondere Erklärungen zum Datenschutz, z. B. über die nach §§ 5 und 6 BDSG getroffenen Vorkehrungen. Ich habe darüber

hinaus empfohlen, von den jeweiligen Forschungsnehmern zu verlangen, daß diese z. B. bei der Erhebung personenbezogener Daten eine Begründung für die Erforderlichkeit des Personenbezugs abgeben. In Fällen, in denen ein Personenbezug erforderlich ist, sollte sich die Bundesanstalt die Erhebungsunterlagen, insbesondere Anschreiben und Aufklärungshinweise vorher zur datenschutzrechtlichen Beurteilung vorlegen lassen.

Eingehend habe ich mich auch mit dem Projekt „Örtliche Unfallforschung" befaßt, bei dem seit Jahren mit Hilfe eines detaillierten Fragebogens zum Teil hochsensible Daten gesammelt und ausgewertet werden. Dazu erhält das Forschungsteam Angaben von öffentlichen und privaten Stellen (z. B. Polizei, Schrotthändlern), aber auch von Trägern besonderer Geheimhaltungspflichten (Arzt, Krankenhaus). Aufgrund meines jetzigen Kenntnisstandes kann ich nicht ausschließen, daß medizinische Daten unter Mißachtung der ärztlichen Schweigepflicht an das Forschungsteam gelangen. Ich habe deshalb die Bundesanstalt um Mitteilung weiterer Einzelheiten gebeten.

2.7.5 Wasser- und Schiffahrtsverwaltung des Bundes

Meine Kontrolle der Wasser- und Schiffahrtsverwaltung des Bundes habe ich mit einem Besuch der Wasser- und Schiffahrtsdirektion (WSD) Mitte in Hannover im Jahre 1982 begonnen. Automatisierte Datenverarbeitung findet bei der WSD Mitte lediglich im Bereich der Lohnrechnungsstelle statt; darüber hinaus ist die WSD an der Pilotanwendung des Personal-Verwaltungs-Systems der Wasser- und Schiffahrtsverwaltung, das zentral bei der Bundesanstalt für Wasserbau in Karlsruhe geführt wird, mittels eines Terminalanschlusses beteiligt.

Gemäß § 12 der Verordnung über das Führen von Sportbooten auf den Binnenschiffahrtsstraßen vom 21. März 1978 (BGBl I S. 420) haben der Deutsche Motoryachtverband, der Deutsche Seglerverband sowie die Strom- und Schiffahrtspolizeibehörden und die Wasserschutzpolizei der WSD Mitte „alle Tatsachen ..., die eine Entziehung des amtlich vorgeschriebenen Befähigungsnachweises oder ein Fahrverbot rechtfertigen können", mitzuteilen. Der Bundesminister für Verkehr hat im Jahre 1981 klargestellt, daß nur rechtskräftige Verurteilungen oder Ordnungswidrigkeiten-Entscheidungen mitzuteilen und zu registrieren sind. Die WSD Mitte sammelt diese Entscheidungen — nach Namen geordnet — in einem Aktenhefter. Die Anzahl der Mitteilungen, die seit dem Inkrafttreten der Verordnung am 1. April 1978 eingegangen sind, ist gering. Sportbootführerscheine wurden offenbar überhaupt noch nie aufgrund von Mitteilungen über Ordnungswidrigkeitenverfahren entzogen. Ich habe daher Zweifel an der Erforderlichkeit dieser Datensammlung geäußert. Der Bundesminister für Verkehr will gleichwohl daran festhalten.

Ich habe weiter bemängelt, daß weder für diese Vorgänge noch für Bußgeldentscheidungen, welche die WSD Mitte nach dem Gesetz über die Aufgaben des Bundes auf dem Gebiet der Binnenschiffahrt erläßt, Tilgungsregelungen bestehen. Der Bundesminister für Verkehr beabsichtigt nunmehr, die Aufbewahrung der entsprechenden Bußgeldakten und der Entscheidungen durch Erlaß auf zehn Jahre zu begrenzen, sofern nicht besondere Gründe eine längere Aufbewahrung gebieten. Ich halte diese Frist jedenfalls bei Entscheidungen in Ordnungswidrigkeitenverfahren für zu lang. Meines Erachtens sollte die Tilgungsregelung des Bundeszentralregistergesetzes als Maßstab herangezogen werden, das z. B. für Verurteilungen zu einer Geldstrafe von nicht mehr als 90 Tagessätzen eine Tilgungsfrist von fünf Jahren vorschreibt. Ich habe dem BMV zudem empfohlen, bei der Registrierung der Tatsachen, die eine Entziehung des Sportbootführerscheines oder ein Fahrverbot rechtfertigen können, die Tilgungsregelungen für das Verkehrszentralregister des Kraftfahrt-Bundesamtes zugrunde zu legen.

2.7.6 Bundesanstalt für Flugsicherung (BFS)

Im letzten Jahr habe ich die Bundesanstalt für Flugsicherung und ihre Außenstelle, die Flugsicherungs-Regionalstelle Frankfurt, einer datenschutzrechtlichen Kontrolle unterzogen. Neben Fragen der Organisation des Datenschutzes und der Datensicherung standen die Datenverarbeitung im Rahmen des Auswahlverfahrens für den gehobenen Flugverkehrskontrolldienst und die Verarbeitung von Daten über die Tätigkeit des Flugverkehrskontrolldienstes im Vordergrund der Prüfung.

Bei dem Auswahlverfahren für den gehobenen Flugverkehrskontrolldienst arbeitet die BFS mit der Deutschen Forschungs- und Versuchsanstalt für Luft- und Raumfahrt e. V. (DFVLR) zusammen. Die DFVLR führt für die BFS Auswahltests mit den Bewerbern durch und legt das Ergebnis einer Auswahlkommission der BFS vor. Klärungsbedürftig waren hierbei insbesondere der Umfang der Datenerhebung — dazu gibt es einen Fragebogen der DFVLR —, die Auswertung und Nutzung der Daten durch die DFVLR und die Übermittlung der Bewerberdaten zwischen der BFS und der DFVLR. Eine erste Stellungnahme der BFS zu meinen Feststellungen brachte noch nicht abschließende Klarheit zu diesen Fragen.

Die Tätigkeit der Mitarbeiter im Flugverkehrskontrolldienst wird durch Daten-, Sprach- und Bildaufzeichnung in nahezu allen Einzelheiten festgehalten. Dies ist notwendig, um die Flugsicherung richtig und kontrollierbar durchführen zu können. Die Aufzeichnungen sind allerdings ohne unmittelbaren Zusammenhang mit Fragen der Luftsicherheit auch dazu geeignet, das Verhalten der Mitarbeiter unter disziplinären Gesichtspunkten zu beurteilen. Eine solche Verwendung hat sich die Bundesanstalt ausdrücklich vorbehalten und hierüber eine Dienstvereinbarung mit dem Gesamtpersonalrat abgeschlossen.

Die Verwertung dieser Aufzeichnungen für Zwecke der Personalführung oder -wirtschaft ist nicht von ihrem ursprünglichen Zweck gedeckt. Eine zweckfremde Nutzung ist zwar nicht von vornherein un-

zulässig, doch ist eine besondere rechtliche Begründung erforderlich, weil diese Aufzeichnungen im Bereich des Flugverkehrskontrolldienstes zu einer so intensiven Kontrolle der Mitarbeiter führen können, wie sie in anderen Bereichen unbekannt ist. Keine unmittelbare Auswirkung auf die datenschutzrechtliche Beurteilung hat die Frage, ob die erwähnten Aufzeichnungsverfahren der Mitbestimmung nach dem Personalvertretungsrecht unterliegen. In kollektivrechtlichen Regelungen wie in der erwähnten Dienstvereinbarung können allerdings Verwendungsmodalitäten festgelegt werden, die die Konflikte mit dem Persönlichkeitsrecht der Betroffenen mildern oder ausräumen. Ich werte die Dienstvereinbarung deshalb positiv, habe der Bundesanstalt jedoch empfohlen, die Bestimmungen zur Löschung und zur Information der betroffenen Bediensteten zu präzisieren. Die BFS hat zugesagt, meine Überlegungen zu berücksichtigen.

2.8 Wissenschaftliche Forschung

2.8.1 Überblick

Ich habe die Einhaltung datenschutzrechtlicher Vorschriften auch bei solchen Stellen des Bundes überprüfen lassen, die Forschung betreiben. Dabei sind jedoch in der Regel keine Mängel festgestellt worden, die speziell dadurch begründet waren, daß es sich um Forschungseinrichtungen handelte. Meine Prüfungserfahrungen sind in diesem Bereich aber kaum repräsentativ, weil die meisten Forschungseinrichtungen von den Ländern unterhalten werden und deshalb von den Landesbeauftragten für den Datenschutz zu überprüfen sind.

Forschungsspezifische Probleme haben sich für mich vielmehr aus kritischen Äußerungen von Wissenschaftlern ergeben, Wissenschaft und Forschung würden durch den Datenschutz unverhältnismäßig beeinträchtigt.

Die Vorwürfe sind leider nur selten substantiiert vorgetragen und durch konkrete Fälle von Beeinträchtigungen belegt worden. Vielfach wurden die Probleme in der Öffentlichkeit vergröbert und polemisch zugespitzt dargestellt, deshalb habe ich teilweise öffentlich erwidert.

Es gibt jedoch auch Stellen, die die Probleme sehr differenziert und ausgewogen darstellen, so z. B. der Wissenschaftsrat in seiner „Stellungnahme zu Forschung und Datenschutz“. Diese Stimmen machen deutlich, daß der Zugang zu den für wissenschaftliche Vorhaben benötigten personenbezogenen Daten tatsächlich schwieriger geworden ist. Jedoch beruhen diese Schwierigkeiten nur in ganz wenigen Fällen wirklich auf Anforderungen des Datenschutzes oder sind nach bestehender Rechtslage unvermeidbar.

Häufig wird der Datenschutz nur als Vorwand genutzt, wenn man die Daten aus anderen Gründen nicht herausgeben will; in anderen Fällen können die Schwierigkeiten durch Anonymisierung gelöst werden; vielfach beruhen sie auch nicht auf den Datenschutzgesetzen, sondern auf speziellen Geheimhaltungsvorschriften oder Berufsgeheimnissen (vgl. Nr. 2.8.3 dieses Berichts).

Die bei der Anwendung des geltenden Rechts bestehenden Schwierigkeiten haben dazu geführt, daß eine sachgerechte Spezialvorschrift für die Datenverarbeitung zu wissenschaftlichen Zwecken in das BDSG aufgenommen werden soll. Eine solche Wissenschaftsklausel wird allseitig als eine wichtige Regelungsaufgabe für die Novellierung des BDSG angesehen (s. dazu Nr. 6.2.5 dieses Berichts).

Die baden-württembergische Landesregierung beabsichtigt sogar — zu weitgehend — bei der Novellierung des Landesdatenschutzgesetzes eine generelle Durchbrechung der seit alters her bestehenden Berufs- und besonderen Amtsgeheimnisse für Forschungszwecke. Bei dieser Gelegenheit soll auch noch eine generelle Ermächtigung zur Führung von Krankheitsregistern in das Gesetz aufgenommen werden (s. auch dazu Nr. 2.8.3).

Ich bin den konkret erkennbaren Problemen der Forschung nachgegangen und habe sie zusammen mit den Datenschutzbeauftragten der Länder analysiert. Die Konferenz der Datenschutzbeauftragten hat Stellungnahmen zu Forschungsbereichen abgegeben, die kurzfristig geregelt werden sollten, beispielsweise zu den geplanten Krebsregistern und zum Psychiatrieprogramm der Bundesregierung. Außerdem habe ich auf Wunsch beteiligter Forschungseinrichtungen konkrete länderübergreifende Datenschutzprobleme, die bei einzelnen Forschungsvorhaben entstanden waren, mit den Landesbeauftragten diskutiert.

Zur Lösung der Probleme habe ich Vorschläge für die Novellierung des BDSG gemacht und in vielen Fällen Anregungen gegeben, wie die Probleme unter dem geltenden Recht vermieden oder gemildert werden können. Ich habe aber auch darauf hingewiesen, daß der Gesetzgeber einige Beschränkungen beim Datenzugang zum Schutze der Betroffenen bewußt in Kauf genommen hat und daß es deshalb jetzt nicht nur darum gehen könne, vermeintlich unbillige Hindernisse wegzuräumen.

2.8.2 Überprüfung von Forschungseinrichtungen

Bei einigen Stellen des Bundes, die Forschung betreiben, habe ich — teilweise nicht unerhebliche — Mängel in der Organisation des Datenschutzes festgestellt. Eine ausreichende Übersicht über die geführten Dateien war häufig nicht vorhanden. Verantwortlichkeiten waren teilweise nicht geklärt. In einem Fall war sogar unklar, welche Institute und welche Personen dort zu welchen Zwecken auf welche Daten zugreifen dürfen. In einem anderen Fall bestehen Zweifel, ob die Einwilligung der Betroffenen in die Verarbeitung ihrer medizinischen Daten immer vorgelegen hat. In der Zwischenzeit sind die meisten Mängel beseitigt worden.

2.8.3 Überprüfung der Datenschutzhindernisse für die Forschung

Durch das Bundesdatenschutzgesetz nicht veranlaßte Einschränkungen für die Forschung

In den zahlenmäßig weitaus überwiegenden Fällen stand der Datenschutz (bei richtiger Beurteilung) dem Datenzugang nicht im Wege. Die Behinderungen beruhten vielmehr oft auf mangelnder Bereitschaft der datenbesitzenden Stelle, Arbeit oder Verantwortung zu übernehmen oder das Projekt zu unterstützen; das Argument „Datenschutz" diente als Ausrede oder Vorwand.

Ich habe bei jeder sich bietenden Gelegenheit darum gebeten, mir alle Fälle zu benennen, in denen der Verdacht besteht, daß Datenschutzvorschriften falsch angewendet werden. Ich habe auch darauf hingewiesen, daß solche Mißstände von den Forschern häufig nur erkannt werden können, wenn sie sich auch selbst mit den einschlägigen Datenschutzvorschriften vertraut machen, und meine Hilfe dazu angeboten.

Wissenschaftsrat, Historiker und Sozialforscher haben beklagt, daß die Übermittlung von Daten in vielen Fällen auch dann „aus Datenschutzgründen" versagt wurde, wenn das BDSG nicht anwendbar sei, etwa bei Daten von Verstorbenen oder bei Daten, die nicht in Dateien gespeichert seien. Zugangshindernisse können sich jedoch in solchen Fällen aus speziellen Geheimhaltungsvorschriften ergeben. Diese stellen regelmäßig nicht darauf ab, ob die betroffenen Personen noch leben oder in welcher Form die Daten verarbeitet werden. Der Ausgangspunkt dieser Regelungen ist vielmehr die besondere Sensitivität bestimmter Daten und ihr Verwendungszusammenhang. Wenn weder die Datenschutzgesetze noch spezielle Geheimhaltungsvorschriften eingreifen, sind Datenübermittlungen zu Forschungszwecken in aller Regel zulässig. Nur ausnahmsweise bei extremen Beeinträchtigungen wird das verfassungsrechtlich garantierte allgemeine Persönlichkeitsrecht entgegenstehen. Es verbietet z. B. die Übermittlung personenbezogener Daten für Forschungsvorhaben, deren Methoden oder Ziele die Ehre des Betroffenen verletzen. Dasselbe gilt, wenn durch ein Forschungsvorhaben das Intimleben der Betroffenen öffentlich zur Schau gestellt würde. Auch wenn eine Person verstorben ist, verbietet das Grundgesetz die Verletzung ihrer Menschenwürde. Eine freie Entfaltung der Persönlichkeit zu Lebzeiten setzt voraus, daß ein gewisser Schutz auch nach dem Tode verbürgt ist. Dieser Schutz wird allerdings mit dem Zeitablauf immer schwächer und erlischt schließlich irgendwann.

Für eine falsche Anwendung der Übermittlungsvorschriften des BDSG dürfte häufig aber auch Rechtsunsicherheit der Stellen, die über die Daten verfügen, die Ursache gewesen sein. Gerade wenn es um die Übermittlung zu Forschungszwecken geht, ist die sachgerechte Anwendung dieser Vorschriften nicht einfach. Ich habe wiederholt darauf hingewiesen, daß die vom BDSG getroffene Unterscheidung zwischen Übermittlungen an öffentliche und solchen an nicht-öffentliche Stellen für Datenübermittlungen zu Forschungszwecken nicht sachgerecht ist. Vielmehr ist eine einheitliche Regelung geboten, die die besonderen Verhältnisse im Bereich der Wissenschaft berücksichtigt und einen Ausgleich zwischen dem Schutz der Betroffenen und der Forschungsfreiheit schafft (s. Nr. 6.5 dieses Berichts).

Alternativen zu unzulässigen Datenübermittlungen

In einigen Fällen hätten die Zugangsprobleme durch *Anonymisierung* der Daten gelöst werden können. Ich habe immer wieder darauf hingewiesen, daß eine faktische Anonymisierung regelmäßig ausreicht. Ab wann Daten dementsprechend so anonymisiert sind, daß Datenempfänger und zugangsberechtigte Dritte einen Personenbezug mit vertretbarem Aufwand nicht mehr herstellen können, ist eine Frage des Einzelfalls. Diese Einzelfallentscheidung setzt eine Prognose zukünftiger möglicher Gefahren voraus. Trotzdem muß die Entscheidung nachvollziehbar und frei von Willkür sein.

Die Anonymisierung wird auch nach Einfügung einer Wissenschaftsklausel in das BDSG ihre Bedeutung behalten. Denn die Nutzung personenbezogener Daten für Forschungszwecke soll nur erlaubt sein, wenn anonymisierte Daten nicht genügen. Außerdem muß dann regelmäßig die Einwilligung der Betroffenen vorliegen; für den Fall, daß diese Einwilligung nicht eingeholt werden kann, soll die Nutzung nur zulässig sein, wenn sie keine schutzwürdigen Belange des Betroffenen beeinträchtigt.

Im Gegensatz zum Wissenschaftsrat halte ich es nicht für angemessen, die Datenschutzvorschriften dahin gehend zu ändern, daß personenbezogene Daten von Anfang an als nicht personenbezogen anzusehen sind, wenn der Datenempfänger sie nach Erhalt anonymisieren will. Die Anonymisierungsabsicht kann allerdings im Einzelfall die Annahme rechtfertigen, daß durch die Datenübermittlung schutzwürdige Belange von Betroffenen nicht beeinträchtigt werden.

Wenn anonymisierte Daten für ein Forschungsvorhaben nicht brauchbar sind und die Übermittlung personenbezogener Daten aus Datenschutzgründen unzulässig ist, bleibt unter Umständen außerdem noch die Möglichkeit, daß die speichernde Stelle die personenbezogenen Daten nach Anweisung der Forscher verarbeitet und dann nur die nicht mehr personenbezogenen Ergebnisse übermittelt.

Eine Anonymisierung mit den heute bekannten Methoden wird schwieriger und unter Umständen unmöglich, wenn Daten in starker Tiefengliederung und auf kleine geographische Einheiten bezogen benötigt werden. Denn dann ist die Wiederherstellung des Personenbezuges vielfach ohne unverhältnismäßigen Aufwand möglich. Diese Situation besteht nach Schilderung des Bundesgesundheitsamtes teilweise bei Forschungsvorhaben im Bereich der Krankheitsursachenforschung.

Weil die derzeitigen Grenzen der Anonymisierung schon frühzeitig deutlich wurden, habe ich mich von Anfang an für die Fortentwicklung von Anonymisierungsverfahren eingesetzt. Die Gesellschaft für Mathematik und Datenverarbeitung (GMD) hat meine Anregung aufgegriffen und betreibt mit Förderung des Bundesministers für Forschung und Technologie und unter Beteiligung des Statistischen Bundesamtes ein entsprechendes Forschungsvorhaben. Zwei Vertreter des Datenschutzes gehören dem Projektbeirat an. Mit dem Forschungsvorhaben soll die Möglichkeit eröffnet werden, nicht nur statistische Ergebnisse, sondern auch Einzelangaben zur Verfügung zu stellen, die folgende Eigenschaften besitzen sollen:

— Die Daten sollen soweit anonymisiert sein, daß die Wiederherstellung des Personenbezuges mit vertretbarem Aufwand nicht möglich ist,

— sie sollen trotzdem möglichst fein gegliederte, also nicht oder nur in geringem Umfang aggregierte Informationen enthalten (Mikrodaten),

— ihre Aussagekraft und -genauigkeit und die Auswertungsmöglichkeiten sollen möglichst wenig eingeschränkt werden, z. B. sollen die Daten miteinander verknüpft werden können, auch soweit sie verschiedene Bereiche betreffen.

Probleme mit dem Einwilligungserfordernis

Nach § 3 BDSG ist eine gesetzlich nicht ausdrücklich erlaubte Verarbeitung personenbezogener Daten nur zulässig, wenn der Betroffene in sie eingewilligt hat. Bei der Erhebung von Daten ist es im Bereich der Sozialforschung nach Angaben der Forscher unter Umständen schwierig, die schriftliche Einwilligung der Betroffenen für die vorgesehenen Datenverarbeitungsmaßnahmen einzuholen. Außerdem wehren sich die Forscher dagegen, eine neue Einwilligung einholen zu sollen, wenn sie Daten später noch zu anderen Forschungszwecken als ursprünglich vorgesehen verwenden. Vergleichbare Probleme habe ich früher schon im Bereich des Bundesministers für Verkehr festgestellt. Mit dem Bundesminister für Verkehr habe ich Richtlinien zur Anpassung der empirischen Forschung an die Bestimmungen des Bundesdatenschutzgesetzes erarbeitet, die diese Probleme für den dortigen Geschäftsbereich weitgehend lösen. Die Richtlinien machen deutlich, daß es vorrangig darauf ankommt, die Betroffenen vor Erteilung der Einwilligung angemessen darüber zu unterrichten, was mit ihren Daten geschieht (vgl. Anhang 1 zu meinem 3. TB S. 63 ff.). Ich habe immer wieder meine Bereitschaft bekundet, an vergleichbaren Richtlinien für andere Bereiche beratend mitzuwirken. Leider ist dieses Angebot bisher nicht in Anspruch genommen worden.

Datenzugangsprobleme für die Forschung infolge bereichsspezifischer Datenschutzvorschriften

Bei den ganz wenigen Fällen, in denen die Zugangsprobleme nicht lösbar erschienen, waren fast nie Bundes- oder Landesdatenschutzgesetze hinderlich, sondern seit langem bestehende Geheimhaltungsvorschriften und Berufsgeheimnisse.

Dennoch habe ich mich — vom Innenministerium Baden-Württemberg um Stellungnahme ersucht — gegen die dortige Absicht gewandt, für Forschungszwecke eine generelle Freistellung von speziell geregelten Geheimhaltungspflichten in das Landesdatenschutzgesetz aufzunehmen. Der Betroffene muß die Gewißheit haben, daß seine persönlichen Angaben in bestimmten Bereichen streng vertraulich behandelt werden. Die speziell geregelten Geheimhaltungspflichten schaffen nämlich erst das Vertrauen, das notwendig ist, um unverzichtbare Informationsbeziehungen zu gewährleisten. Beispiele, die keiner näheren Erläuterung bedürfen, sind Arztgeheimnis, Anwaltsgeheimnis, Statistikgeheimnis, Steuergeheimnis. Eine Durchbrechung dieser Geheimnisse kann deshalb nur in Einzelfällen, die für den Betroffenen in ihren konkreten Auswirkungen überschaubar bleiben, unter folgenden Voraussetzungen angemessen sein:

— Die Durchbrechung dient einem Zweck von überragender Bedeutung,

— dieser Zweck kann ohne personenbezogene Daten nicht erreicht werden und

— es ist unmöglich, die Einwilligung des Betroffenen einzuholen, oder der überragende Zweck ist nicht erreichbar, wenn die Entscheidung den einzelnen Betroffenen überlassen bleibt.

So wird man von der Einwilligung des Betroffenen absehen können, wenn ein nicht belastbarer Patient zu seinem eigenen Schutz nicht umfassend über seine Krankheit aufgeklärt werden darf. Der ohne personenbezogene Daten nicht erreichbare Zweck von überragender Bedeutung kann vielleicht vorliegen, wenn die Ursachen einer bestimmten schweren Krankheit untersucht werden müssen.

Jede einzelne Durchbrechung eines Berufs- oder besonderen Amtsgeheimnisses verlangt aber zunächst eine genaue Prüfung, ob sie mit den Bedürfnissen und Funktionen vereinbar ist, denen gerade dieses Geheimnis dient. Solche Prüfungen haben — soweit ersichtlich — noch nicht stattgefunden. Sie sind jedoch unabdingbar, soll nicht in Kauf genommen werden, daß höchst empfindliche Vertrauensverhältnisse erschüttert und geschützte Kommunikationsbeziehungen geschädigt werden.

2.9 Archivwesen

In meinem Zweiten (S. 14) und Vierten Tätigkeitsbericht (S. 50) hatte ich auf die Erforderlichkeit eines Bundesarchivgesetzes hingewiesen. Auch von seiten der Archivverwaltung wird dies erkannt, weil Datenschutzvorschriften unter bestimmten Voraussetzungen die Vernichtung von Unterlagen gestatten oder sogar gebieten. Im Interesse der Archive und der Archivnutzung ist deshalb zunächst die Pflicht zur Abgabe nicht mehr erforderlicher Unterlagen an das Archiv zu regeln. Dazu muß von daten-

schutzrechtlichen Löschungsvorschriften abgegangen werden; es ist dann aber auch notwendig, den Schutz der Betroffenen durch spezielle Vorschriften auf andere Weise, insbesondere durch eingeschränkte Zugänglichkeit der Unterlagen im Archiv, zu sichern.

Auf der Grundlage dieser Überlegungen ist ein Referentenentwurf für ein Bundesarchivgesetz entstanden. Die Regelungen erscheinen sachgerecht. Einige Vorschriften berücksichtigen die Belange der Betroffenen allerdings noch nicht angemessen.

Ein datenschutzrechtliches Problem besteht nach wie vor darin, daß durch die Abgabeverpflichtungen der speichernden und aktenführenden Stellen gegenüber dem Bundesarchiv die Löschungspflichten dieser Stellen auch für solche Unterlagen nur verzögert erfüllt werden können, die später vom Archiv gar nicht übernommen werden. In diesem Zusammenhang ist vor allem § 2 Satz 1 des Gesetzentwurfes problematisch, der regelt, daß die Unterlagen nicht in jedem Fall schon dann dem Bundesarchiv zur Übernahme anzubieten sind, wenn sie zur Erfüllung der Aufgaben der abgebenden Stellen nicht mehr benötigt werden, sondern gegebenenfalls erst dann, wenn ihre Aufbewahrung an der bisherigen Stelle nicht mehr zur Wahrung der Sicherheit der Bundesrepublik Deutschland erforderlich ist. Diese Regelung wurde eingefügt, um Sicherheitsbedenken gegen eine frühzeitige Kenntnisnahme des Inhalts besonders empfindlicher Unterlagen durch Angehörige des Bundesarchivs zu beseitigen. Andererseits wird es den Behörden dadurch ermöglicht, noch auf Unterlagen zuzugreifen, die sie unter Datenschutzgesichtspunkten hätten löschen müssen. Notwendig ist deshalb eine Regelung, die einen unkontrollierten Zugriff sowohl seitens der abgebenden als auch seitens der übernehmenden Stelle für den fraglichen Übergangszeitraum verhindert. Einen entsprechenden Vorschlag habe ich gemacht.

Um der Gefahr zu begegnen, daß datenschutzrechtliche Löschungspflichten zu spät erfüllt werden, habe ich auch vorgeschlagen, in § 4 des Gesetzentwurfes eine so frühzeitige Anbietung der Unterlagen vorzuschreiben, daß die Übernahme — jedenfalls dann, wenn keine Sicherheitsbelange entgegenstehen — vor Eintritt der Löschungsverpflichtung abgeschlossen sein kann.

Damit die datenschutzrechtlichen Löschungsgebote nicht völlig leerlaufen, sollte auch vorgesehen werden, daß die Übernahme vollständiger Bestände ganzer Verwaltungsbereiche (wie das z. B. für die Lastenausgleichsunterlagen vorgesehen ist) nur auf der Grundlage eines Gesetzes zulässig ist.

Es besteht Einvernehmen, daß die schutzwürdigen Belange der Betroffenen weitgehend durch allgemeine Benutzungssperrfristen, die sich nach Güterabwägung im Einzelfall verlängern oder verkürzen lassen, mit berechtigten Benutzerinteressen in Einklang gebracht werden können. Auf diese Weise dürfte es auch möglich sein, z. B. berechtigte Interessen der zeitgeschichtlichen Forschung zu berücksichtigen, vor allem wenn man die Rechtsprechung zum Persönlichkeitsrecht von Personen der Zeitgeschichte berücksichtigt.

Im Hinblick auf die Löschungspflichten in allgemeinen und bereichsspezifischen Datenschutzvorschriften habe ich Bedenken dagegen erhoben, daß Behörden, denen unbeschränkt Auskunft aus dem Bundeszentralregister zu erteilen ist, allgemein von den Benutzungssperrfristen freigestellt werden sollen. Diese Regelung läßt unbeachtet, daß im Bundesarchiv sehr viel weitergehende Unterlagen vorhanden sind. Sie verstößt aber vor allem gegen den zentralen Datenschutzgedanken des Archivwesens, daß die ausnahmsweise unbegrenzt aufbewahrten Unterlagen nur unter engen und genau kontrollierten Bedingungen genutzt werden dürfen.

Einwendungen habe ich auch gegen die einschränkende Regelung des Benutzungsanspruchs des Betroffenen erhoben. Dieser Anspruch soll nur für Archivgut gelten, das sich nach seiner Zweckbestimmung auf natürliche Personen bezieht. Im übrigen hätte der Betroffene dann nur den allgemeinen Benutzungsanspruch wie jedermann, der jedoch oft nicht zum Ziel führt. Das erscheint mir schon deshalb nicht sachgerecht, weil dann die Möglichkeit bestünde, daß zwar Dritte, z. B. Wissenschaftler, Zugang zu den Daten erhalten, nicht aber der Betroffene selbst.

Ich habe in den letzten Jahren mehrere Informationsbesuche und Bereichsprüfungen im Bundesarchiv durchgeführt. Was die in Archivalien enthaltenen Daten anbelangt, ist das Bundesarchiv seit jeher mit Erfolg bemüht, das Persönlichkeitsrecht der Betroffenen zu wahren. Verschiedentlich habe ich das Bundesarchiv beraten. Im Hinblick auf die während des Dritten Reiches unter Zwang angelegten Sinti-Karteien wurde Einvernehmen erzielt, daß eine personenbezogene Nutzung der darin enthaltenen Informationen ohne Einwilligung der Betroffenen deren schutzwürdige Belange verletzen würde.

2.10 Statistik

In den letzten Jahren habe ich mehrfach die Organisation des Datenschutzes im Statistischen Bundesamt in Wiesbaden sowie seiner Außenstelle in Berlin überprüft. Die dabei festgestellten Mängel wurden in der Zwischenzeit weitgehend behoben.

Auf die Durchführung der meisten Bundesstatistiken kann ich nur mittelbar Einfluß nehmen, da sie vorwiegend den Ländern obliegt. Das Statistische Bundesamt hat nach § 3 Bundesstatistikgesetz (BStatG) die Bundesstatistiken zwar vorzubereiten, kann seiner Aufgabe, auf eine einheitliche Durchführung hinzuwirken, weitgehend aber nur durch Empfehlungen an die Länder nachkommen. Ich habe mich deshalb besonders der Koordination des Datenschutzes im Rahmen des Erfahrungsaustausches zwischen den Datenschutzbeauftragten gewidmet.

In einem Arbeitskreis, dem ich vorsitze, wurden beispielsweise mehrere Statistiken nach Merkmalskatalog und Tiefengliederung auf ihre Gesetzmäßigkeit und — im Lichte des Mikrozensus-Beschlusses des Bundesverfassungsgerichts — auf ihre Verfassungsmäßigkeit überprüft. Dabei habe ich mich an den vom Bundesverfassungsgericht (vgl. BVerfGE 27, 1, 6 f. und 344, 350 ff.) aufgestellten Grundsätzen zu den Grenzen statistischer Befragungen orientiert.

Im Jahre 1980 hatte ich Bedenken dagegen erhoben, daß den Statistischen Ämtern für die Wanderungsstatistik nach § 6 Abs. 1 des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes die vollständigen Meldescheine der Meldebehörden zugeleitet werden. Denn die Meldescheine enthalten mehr Daten, als für die Durchführung der Statistik erforderlich ist. Diesen Bedenken will der Bundesminister des Innern bei der Novellierung des Gesetzes Rechnung tragen.

Zusammen mit den Landesbeauftragten für den Datenschutz habe ich die Verfahren einzelner Statistiken daraufhin überprüft, ob der nach den Erhebungsunterlagen vorgesehene Merkmalskatalog von den einschlägigen Statistikgesetzen gedeckt ist. Die gesetzlichen Ermächtigungen sind m. E. grundsätzlich eng auszulegen, weil der Bürger in der Regel unter Bußgeldandrohung zur Beantwortung der Statistikfragen verpflichtet ist, der Staat also unter Zwang in seine Privatsphäre eingreift. Unter diesen Gesichtspunkten wurden Bedenken gegen die Erhebung von Identifikationsmerkmalen für die Jahresstatistik der Sozialhilfe geltend gemacht. Die Statistischen Ämter haben daraufhin auf die Erhebung dieser Daten verzichtet.

Zur Zeit wird geprüft, ob der in den Erhebungsbögen für die Bundesstatistik der Rehabilitationsmaßnahmen vorgesehene Merkmalskatalog in der vorgesehenen Tiefengliederung unter Berücksichtigung des Mikrozensusbeschlusses des Bundesverfassungsgerichts von § 51 des Schwerbehindertengesetzes gedeckt ist.

Die Landesbeauftragten für den Datenschutz und ich haben wiederholt auch darauf hingewiesen, daß der Erhebungsweg für Bundesstatistiken nach Möglichkeit so gestaltet werden muß, daß schon der Verdacht, ein Bruch des Statistikgeheimnisses sei möglich, nicht entstehen kann. Einzeleingaben zeigen aber, daß Bürger fürchten, ihre Angaben könnten zu ihrem Nachteil auch zu Verwaltungszwecken genutzt werden. Das ist vor allem dann der Fall, wenn an der statistischen Erhebung Stellen beteiligt sind, die die gleichen Angaben auch für Verwaltungsentscheidungen benötigen. Ein Landwirt beklagte sich z. B. bei mir, seine Heimatgemeinde habe seine Angaben zur Größe des Schweinebestandes aus den Unterlagen für die statistische Viehzählung bei der Entscheidung über eine Baugenehmigung berücksichtigt. Die zuständige Datenschutzkontrolleinrichtung konnte dies zwar nicht feststellen, aus der Sicht des Bürgers ist aber ein solcher Argwohn gerade bei kleinen Gemeinden, wo viele Aufgaben von derselben Person wahrgenommen werden, durchaus berechtigt.

Zum Schutze des Betroffenen wird die Pflicht zur Geheimhaltung durch die Pflicht ergänzt, alle Daten, die der Identifizierung der Betroffenen dienen, zu löschen, sobald ihre Kenntnis für die Erfüllung von Aufgaben auf dem Gebiet der Bundesstatistik nicht mehr erforderlich ist (§ 11 Abs. 7 BStatG). Aus diesem Grunde müssen die von den Statistischen Ämtern festgelegten Mindestaufbewahrungsfristen für statistisches Material insoweit als Höchstaufbewahrungsfristen angesehen werden. Ich habe das Statistische Bundesamt gebeten, mir mitzuteilen, wie die Löschung der Daten nach diesen Fristen im Statistischen Bundesamt gewährleistet wird, und zusammen mit den Statistischen Landesämtern zu prüfen, ob die Fristen verkürzt werden können.

In meinem Vierten Tätigkeitsbericht (S. 49) hatte ich empfohlen, die Beantwortung von statistischen Fragen für Repräsentativstatistiken nicht mehr — unter Bußgeldandrohung — zur Pflicht zu machen, sondern sie freizustellen, wie das im Ausland vielfach üblich ist. Leider ist dieser Empfehlung bei der Novellierung des Mikrozensusgesetzes nur hinsichtlich einzelner Fragen entsprochen worden. Viele Eingaben zeigen aber den Unmut der Betroffenen darüber, daß unter Zwang in die Privatsphäre eingedrungen wird. Ich meine nach wie vor, daß die Freiwilligkeit der Auskünfte bei entsprechender Aufklärung über die Bedeutung der Statistik die statistischen Ziele nicht gefährden würde.

2.11 Sozialverwaltung

2.11.1 Problemüberblick

Steigende Aufwendungen für den Sozialhaushalt bei sinkenden Beschäftigungszahlen stellen die Sozialverwaltungen vor schwierige, kaum lösbare Probleme. Unbestritten sind einige Maßnahmen und Ziele, mit denen die Folgen zu geringen Wachstums aufgefangen werden müssen:

- Kostensenkung und verbesserte Transparenz des Leistungsgeschehens
- Verhinderung des unrechtmäßigen bzw. unbilligen Bezugs von Sozialleistungen
- verstärkter Einsatz der Informationstechnik, wo er sinnvoll ist.

Am Anfang meiner Amtszeit hatte ich Anlaß zu der Befürchtung, daß die Umsetzung dieser schon damals — wenn auch vage — formulierten Ziele sich mit Mitteln vollzieht, die mit dem Anliegen des Datenschutzes nur schwer vereinbar sind. Ich habe dafür folgende Worte gewählt:

> „Ich befürchte, daß der vom System der sozialen Sicherung verwaltete Bürger zunehmend entmündigt und passiviert wird, die unterschiedlichen Träger sozialer Vorsorge zu einem einheitlichen ‚Informationsblock' zusammenwachsen und der schon jetzt auch für Fachleute schwer zu überblickende Bereich der sozialen Sicherung vollends undurchschaubar wird." (2. TB S. 25)

Im allgemeinen haben sich diese Befürchtungen nicht bewahrheitet — zum einen, weil die Realisierung so mancher Automatisierungsvorhaben bei weitem nicht so schnell vorangegangen ist, wie ursprünglich anzunehmen war; zum anderen, weil sich aufgrund der rasant fortschreitenden technologischen Entwicklung die Gefährdungspotentiale der Informationstechnik verschoben haben. Riskant sind nicht allein zentrale Systeme und Dateien, sondern die beliebige Verfügbarkeit personenbezogener Daten, in welcher technischen Organisationsform auch immer. Außerdem haben die bereichsspezifischen Datenschutzregeln des SGB X dazu beigetragen, das Bewußtsein für die Notwendigkeit disziplinierten Umgangs mit personenbezogenen Daten zu schärfen. Für besonders hilfreich halte ich die Vorschrift des § 96 Abs. 3 SGB X (sie tritt am 1. Juli 1983 in Kraft), die die Bildung einer „Zentraldatei mehrerer Leistungsträger für Daten der ärztlich untersuchten Leistungsempfänger" für unzulässig erklärt — eine Vorschrift, die problematischen Entwicklungen entgegenwirken könnte.

Diesen zu vorsichtigem Optimismus berechtigenden Entwicklungen stehen nach wir vor Tendenzen gegenüber, die ich für bedenklich halte:

Verwendung der Rentenversicherungsnummer außerhalb der Rentenversicherung

Die Rentenversicherungsnummer ist aus meiner Sicht ein geeignetes Organisationsmittel, große Datenbestände zu ordnen und einzelne Datensätze wiederzufinden. Zudem ist sie in der Praxis erprobt, was ihre Anziehungskraft für andere Bereiche als den der Rentenversicherung erklärt. Wie ich unten noch im einzelnen darlegen werde, sehe ich nach wir vor die Gefahr, daß mit dieser Nummer ein Personenkennzeichen für die sozialversicherungspflichtige Bevölkerung (ungefähr 90% der Gesamtbevölkerung) eingeführt wird. Selbst wenn man meinen Risikovermutungen im einzelnen nicht folgen mag, so sollte doch klar sein, daß die Einführung dieser Nummer in andere Bereiche außerhalb der Rentenversicherung nicht auf administrativem Wege, sondern nur durch den Gesetzgeber selbst erfolgen kann (s. auch unten 2.14.8 und 2.15.3).

Standardisierung medizinischer Entscheidungsprozesse

Die Bemühungen, medizinische Entscheidungsprozesse z. B. im REHA-Bereich zu standardisieren, sind vorangeschritten. Daß diese Entwicklung auch vor der Medizin nicht haltmachen kann und soll, ist selbstverständlich. Ich bezweifle aber, ob dieser Bereich, der in hohem Maße vom wechselseitigen Vertrauen von Ärzten und Kranken geprägt sein sollte, mit dem gleichen Maßstab gemessen werden kann wie die Verwaltungsautomation im allgemeinen:

— Die aus vielen Gründen notwendigen Rationalisierungsmaßnahmen müssen hier dazu führen, daß Tätigkeiten, die früher ausschließlich bei Ärzten lagen, jetzt zumindest teilweise von anonymen Systemen und Systemspezialisten übernommen werden. Daß die — theoretisch — entstehenden neuen Spielräume auch tatsächlich für eine bessere Betreuung der Menschen genutzt wurden, habe ich nicht feststellen können.

— Zu dieser unbemerkten Verschiebung in den Verantwortlichkeiten tritt ein weiteres Problem, das schon bei dem noch zu behandelnden Projekt DVDIS, mehr aber noch bei sogenannten Expertensystemen, einem Hauptforschungsgegenstand der modernen Computerwissenschaft, sichtbar wird. Diese Systeme enthalten implizit eine Definition von Krankheit und entsprechend eine Abgrenzung zur Gesundheit. Verkürzungen und Informationsverluste sind unumgänglich, wenn solche Systeme praktikabel sein sollen. Kein noch so guter Raster kann jedoch die Wirklichkeit vollständig abbilden. Es besteht deshalb die Gefahr, daß sich die Definition dessen, was krank und was gesund ist, unmerklich verschiebt. Es gibt eine Grenze, von der an die Automatisierung und die dazu notwendige Formalisierung von medizinischen Entscheidungsprozessen unterlassen werden sollte. Diese Grenze ist zwar schwer zu bestimmen und nicht abstrakt formulierbar, wohl aber in konkreten Fällen erkennbar.

Defizite in der Mitwirkung der Betroffenen bei der Datenerhebung

Das Versichertenverhältnis der sozialversicherten Bürger besteht regelmäßig aus folgenden Elementen:

— der Versicherungs- und Beitragspflicht

— dem Leistungsanspruch

— den Mitwirkungs- und Mitteilungspflichten

— dem Geheimhaltungsanspruch.

Über seine Mitteilungs- und Mitwirkungspflichten ist der Bürger aufzuklären. Dies ergibt sich aus § 9 Abs. 2 BDSG und aus § 66 Abs. 3 SGB I. Die Umsetzung dieser Vorschriften bereitet offensichtlich in vielen Fällen noch immer Schwierigkeiten.

Auf Formularen und Vordrucken, mit denen Sozialleistungsträger in vielfältigen Zusammenhängen vom Bürger Angaben über seine persönlichen und sachlichen Verhältnisse verlangen, fehlt häufig der in § 9 Abs. 2 BDSG vorgeschriebene Hinweis auf die Rechtsvorschrift für die Datenerhebung bzw. auf die Freiwilligkeit der Angaben. In anderen Fällen enthält zwar der Erhebungsvordruck einen „Hinweis gemäß § 9 Abs. 2 BDSG", der jedoch oft nicht dem Inhalt und dem Zweck dieser Vorschrift entspricht. Die Formulierung etwa „Die Angaben sind zur Durchführung des § 205 Abs. 4 RVO erforderlich" versetzt den Betroffenen kaum in die Lage, die Erforderlichkeit der verlangten Angaben tatsächlich nachzuprüfen. Außerdem ist es ihm aufgrund dieses Hinweises überhaupt nicht möglich zu erkennen und einer kritischen Prüfung zu unterziehen, ob er verpflichtet ist, die verlangten Angaben zu machen. Genau dieses soll jedoch durch den — richtig und verständlich formulierten — Hinweis

bewirkt werden. Nach § 9 Abs. 2 BDSG genügt es eben nicht, auf die Erforderlichkeit der Daten hinzuweisen, so bürgerfreundlich und wünschenswert eine Aufklärung über Verwendungszusammenhänge auch ist; vielmehr muß aus dem Hinweis auch hervorgehen, ob die darin genannte Rechtsvorschrift den Betroffenen zur Angabe personenbezogener Daten verpflichtet. Eine solche Vorschrift ist z. B. § 318 a Abs. 1 Satz 4 RVO: „Die Versicherten haben die zur Meldung sowie zur Durchführung der Versicherung und der der Kasse übertragenen Aufgaben erforderlichen Angaben zu machen."

In manchen Fällen besteht für den konkreten Erhebungsanlaß keine ausdrückliche rechtliche Auskunfts- oder Mitteilungspflicht. Dann handelt es sich im Grunde um freiwillige Angaben und der Betroffene ist auf die Freiwilligkeit hinzuweisen.

Diese Freiwilligkeit ist jedoch oft nur scheinbar. Wer Sozialleistungen beantragt oder erhält, hat alle Tatsachen anzugeben, die für die Leistung erheblich sind (§ 60 Abs. 1 Nr. 1 SGB I). Antrags- und Erhebungsvordrucke enthalten deshalb mitunter anstelle des Hinweises gemäß § 9 Abs. 2 BDSG einen Hinweis auf § 60 SGB I. Dieser Hinweis kann aber den vorgeschriebenen Hinweis gemäß § 9 Abs. 2 BDSG wegen der andersartigen rechtlichen und inhaltlichen Qualität des § 60 SGB I nicht ersetzen, sondern allenfalls ergänzen. Denn er besagt nichts darüber, ob der Betroffene verpflichtet ist, die geforderten Angaben zu machen. Er erweckt jedoch beim Betroffenen den unzutreffenden Eindruck einer absoluten Verpflichtung. Tatsächlich handelt es sich um eine Obliegenheit, die stets mit einem Leistungsbegehren einhergeht. Die Nichterfüllung dieser Obliegenheit stellt keine Rechtsverletzung dar, die — wie etwa die Nichterfüllung einer gesetzlichen Auskunftspflicht — als Ordnungswidrigkeit geahndet und somit mit Zwangsmitteln durchgesetzt werden könnte. Die Verletzung der Obliegenheit hat allenfalls negative Auswirkungen auf das Leistungsbegehren des Betroffenen, und auch dies nur unter bestimmten Voraussetzungen; Sozialleistungen dürfen wegen fehlender Mitwirkung nur versagt oder entzogen werden, wenn hierdurch die Aufklärung des Sachverhalts erheblich erschwert wird und nachdem der Leistungsberechtigte auf diese Folge schriftlich hingewiesen worden ist (§ 66 Abs. 1 und 3 SGB I).

Diese auch in Bürgereingaben immer wieder bemängelten Fehler scheinen mir tiefere Ursachen zu haben. Nach wie vor scheint einigen Verwaltungen das Bewußtsein dafür abzugehen, daß sich eine Vielzahl von Kontakten mit den Versicherten fast ausschließlich — wie meist der erste — über Formulare vollzieht. Formulare entscheiden deshalb in erheblichem Umfang darüber, welche Haltung der Bürger gegenüber der Verwaltung einnimmt.

Gelegentlich sind diese Probleme nicht das Ergebnis einer schlechten Verwaltungspraxis, sondern mittelbare Folge gesetzgeberischer Entscheidungen. Ein Beispiel hierfür ist das Rentenanpassungsgesetz 1982 v. 1. Dezember 1981 (BGBl. I S. 1205). Dieses Gesetz überträgt den Krankenkassen neue Aufgaben mit der Folge, daß die betroffenen Rentner eine Fülle persönlicher vermögensbezogener Angaben machen müssen. Eine auffallend große Zahl von Eingaben zeigt mir, daß das gesetzgeberische Ziel von vielen alten Menschen nicht verstanden wurde. Ich kritisiere nicht die Ziele des Gesetzgebers, gebe aber zu bedenken, daß auch eilige gesetzgeberische Entscheidungen mit einer so weitreichenden Erhebung personenbezogener Daten dem Bürger erklärt werden müssen. Dies ist in diesem Fall, auch wenn die Formulare der Kassen meist in Ordnung waren, offensichtlich nicht gelungen.

Einwilligungspostulat

Der Gesetzgeber hat aus gutem Grund die Zulässigkeit der personenbezogenen Datenverarbeitung von der Erlaubnis durch eine entsprechende Rechtsvorschrift und alternativ dazu von der Einwilligung des Betroffenen abhängig gemacht (§ 3 BDSG). Beide Zulässigkeitsvoraussetzungen stehen gleichrangig nebeneinander, keine ist in ihrer rechtlichen Qualität besser oder schlechter. Allerdings gibt es Situationen, in denen der Betroffene faktisch nicht frei über die Einwilligung entscheiden kann, sondern unter psychischem Druck steht, sie zu erteilen; hier ist der gesetzlichen Regelung der Vorzug zu geben, wenn sie — wie regelmäßig — auf einer gründlichen Abwägung der Vor- und Nachteile beruht. Der Rückgriff auf eine Rechtsvorschrift kann für die datenverarbeitende Stelle auch bequemer sein, weil sie für alle gleichartigen Fälle gilt, während eine erforderliche Einwilligung von jedem Betroffenen gesondert eingeholt oder besser erbeten werden muß und möglicherweise auch versagt werden kann. Dies hat der Gesetzgeber jedoch bewußt nicht nur in Kauf genommen, sondern so im BDSG angelegt.

Ich habe mich nie gegen vernünftige gesetzliche Regelungen in spezifischen Bereichen gesträubt, sondern bin in vielen Fällen nachdrücklich dafür eingetreten. Ich muß aber davor warnen, Verrechtlichungsprozesse unnötig voranzutreiben, besonders wenn es um das Selbstbestimmungsrecht des einzelnen über die Offenlegung intimster gesundheitlicher Verhältnisse geht. Vor allem in der medizinischen Forschung gibt es Bestrebungen, von der Einwilligung als Zulässigkeitsvoraussetzung abzukommen und spezielle gesetzliche Erlaubnisse für die Datenverarbeitung zu fordern mit der Begründung, daß tatsächliche oder vermeintliche Schwierigkeiten hinsichtlich des Zugangs zu personenbezogenen Daten andernfalls nicht auszuräumen seien. Forschung, insbesondere medizinische Forschung, sei so wichtig und außerdem verfassungsrechtlich garantiert, daß sie — soweit dafür personenbezogene Daten benötigt werden — nicht von der Bereitschaft der Betroffenen, dazu ihre Einwilligung zu geben, abhängig gemacht werden dürfe. Die Erfahrung zeigt jedoch, daß auch hier interessen- und sachgerechte Lösungen ohne gesetzliche Regelungen auf der Basis der Einwilligung möglich sind (vgl. oben Nr. 2.8.3).

Trotz dieser problematischen Tendenzen kann ich insgesamt feststellen: Datenschutz ist zum festen

Bestandteil der Praxis der Sozialverwaltung geworden. Dies war wegen der langen Tradition des Sozialgeheimnisses und Arztgeheimnisses nicht anders zu erwarten. Mir sind nur wenige Mißbrauchsfälle bekannt geworden, die Anlaß zu förmlichen Beanstandungen gaben. Die Zusammenarbeit mit den einzelnen Trägern ist in der Regel gut.

Angesichts der Vielzahl zu überprüfender Stellen habe ich naturgemäß Schwerpunkte setzen müssen. Meine Arbeitsweise war darauf ausgerichtet, für den Gedanken des Datenschutzes zu werben, Anstöße für betroffenenfreundliche Lösungen zu geben und im günstigsten Fall meine Mitarbeit überflüssig zu machen. Das hat natürlich nicht ausgeschlossen, wo erforderlich, Beanstandungen auszusprechen. Dieses Vorgehen hat sich bewährt. Allerdings sind neue, schwierige Aufgaben auf meine Dienststelle zugekommen. Sie wird zunehmend gebeten, schon bei der Entwicklung neuer Systeme und Verfahren die Belange des Datenschutzes einzubringen. Dieser Herausforderung wird sie sich in Zukunft verstärkt stellen.

2.11.2 Amtshilfe durch Sozialleistungsträger

Das für die öffentlich-rechtliche Verwaltungstätigkeit der Sozialleistungsträger im ersten Kapitel des Zehnten Buches Sozialgesetzbuch (SGB X) von 1980 geregelte Verwaltungsverfahren hat die Vorschriften des Verwaltungsverfahrensgesetzes über die Amtshilfe fast wörtlich übernommen.

Die danach auch von den Leistungsträgern grundsätzlich zu gewährende Hilfe für die Verwaltungstätigkeit anderer Behörden ist allerdings durch die Vorschriften über die Wahrung des Sozialgeheimnisses (§ 35 SGB I) und über den Schutz der Sozialdaten (§§ 67 bis 77 SGB X) beschränkt, soweit damit eine Offenbarung personenbezogener Daten verbunden ist.

Bemerkenswert sind die Regelungen der §§ 72 und 73 über die Offenbarung personenbezogener Daten an die Sicherheitsbehörden und an die Strafverfolgungsbehörden zum Schutz der inneren und äußeren Sicherheit bzw. zur Aufklärung eines Verbrechens oder Vergehens. In beiden Vorschriften wird die Offenbarung personenbezogener Daten an diese Behörden nicht als Amtshilfe bezeichnet, und es wird auch nicht auf die Amtshilfevorschriften Bezug genommen. Aus dem anscheinend beziehungslosen Nebeneinander dieser Vorschriften hat sich eine streitige Diskussion entwickelt, in der zwei Meinungen gegeneinander stehen:

— Die eine Meinung, die auch ich zunächst vertreten habe, sieht die §§ 72, 73 als leges speciales gegenüber den allgemeinen Amtshilfevorschriften des § 68 an. Die Offenbarung von Sozialdaten für Zwecke der inneren und äußeren Sicherheit bzw. der Aufklärung eines Verbrechens oder Vergehens sei in den Spezialvorschriften abschließend geregelt; dies ergebe sich schon daraus, daß die §§ 72, 73 sowohl hinsichtlich der Datenarten als auch hinsichtlich der Zulässigkeitsvoraussetzungen von § 68 abweichen. Die in den Spezialvorschriften angesprochenen Behörden und Stellen könnten ein Offfenbarungsersuchen an einen Leistungsträger daher ausschließlich auf § 72 bzw. § 73 stützen, wobei stets die gegenüber der allgemeinen Amtshilfe strengeren Voraussetzungen erfüllt sein müssen (§ 72: Entscheidung über die Erforderlichkeit durch einen Beauftragten, der die Befähigung zum Richteramt haben soll, Unterrichtung der Aufsichtsbehörde, § 73: richterliche Anordnung). Seien diese Voraussetzungen nicht erfüllt, so sei ein Rückgriff auf § 68 selbst dann nicht möglich, wenn sich das Offenbarungsersuchen lediglich auf die in § 68 genannten Datenarten beschränke.

— Die Gegenmeinung argumentiert wie folgt:

  Der Gesetzgeber habe mit den §§ 72, 73 den dort angesprochenen Stellen über § 68 hinaus zusätzliche Informationsmöglichkeiten eröffnen wollen. Diese Stellen sollten die in § 68 genannten Sozialdaten (neben weiteren Daten) zur Erfüllung ihrer besonders wichtigen öffentlichen Aufgaben auch dann erhalten, wenn Grund zur Annahme besteht, daß durch die Offenbarung schutzwürdige Belange des Betroffenen beeinträchtigt werden, oder wenn sich die ersuchende Stelle die Daten auch auf andere Weise beschaffen könnte. Dieser Erweiterung des Datenumfangs und der Erleichterung ihres Zugangs stünden als Ausgleich die strengeren Voraussetzungen bei der ersuchenden Stelle gegenüber. Seien diese Voraussetzungen bei der ersuchenden Stelle im Einzelfall nicht erfüllt und erstrecke sich das Offenbarungsersuchen ausschließlich auf die in § 68 genannten Datenarten, dann sei die Offenbarung auch im Wege und Rahmen der allgemeinen Amtshilfe des § 68 zulässig. Andernfalls seien diese Stellen ohne ausreichenden Grund schlechter gestellt als alle anderen öffentlichen Stellen, was nicht in der Absicht des Gesetzgebers gelegen haben könne.

Beide Meinungen haben eine Reihe guter und einleuchtender Argumente für sich. Ich neige nach erneutem Überdenken nunmehr eher der zweiten Auffassung zu; die damit in der Praxis zu erreichenden Ergebnisse sind m. E. sachgerecht und unter Datenschutzgesichtspunkten vertretbar:

Benötigen Sicherheitsbehörden oder Strafverfolgungsbehörden lediglich Daten der in § 68 genannten Art und liegen die besonderen Voraussetzungen bei der ersuchenden Stelle nach §§ 72, 73 im Einzelfall nicht vor, dann können auch diese Behörden ein Offenbarungsersuchen an einen Sozialleistungsträger auf § 68 stützen.

Der ersuchte Leistungsträger muß dabei in die Lage versetzt werden, sich ein Urteil darüber zu bilden, ob durch die erbetene Offenbarung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Dafür ist zumindest erforderlich, daß die ersuchende Stelle den Anlaß und den Zweck des Ersuchens nennt. Kann der Leistungsträger diese Beurteilung nicht vornehmen, weil z. B. aus Geheimhaltungsgründen die ersuchende Stelle Anlaß und Zweck des Ersuchens nicht bekanntgeben will oder

kann, dann müßte eine Offenbarung im Wege der Amtshilfe abgelehnt und die ersuchende Stelle auf die Spezialvorschriften der §§ 72 bzw. 73 verwiesen werden mit der Konsequenz, daß eine Offenbarung nur unter den dort genannten Voraussetzungen zulässig ist. Gleiches gilt selbstverständlich, wenn das Ersuchen auf weitere Datenarten als die in § 68 geannnten gerichtet ist.

Auch bei Vorliegen der geschilderten Amtshilfevoraussetzungen ist der ersuchte Leistungsträger zur Offenbarung nicht verpflichtet (aber berechtigt), wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann. Die ersuchende Stelle sollte deshalb in geeigneter Form darlegen, daß sie sich die Angaben auf andere Weise, z. B. durch Anfrage bei der Meldebehörde, nicht beschaffen konnte. In diesem Zusammenhang wurde auch die Auffassung vertreten, als mögliche „andere Weise" sei auch ein Offenbarungsersuchen auf der Grundlage der §§ 72, 73 anzusehen, d. h. der Inanspruchnahme der allgemeinen Amtshilfe durch Sicherheitsbehörden oder Polizei müsse der Versuch vorausgehen, die gewünschte Offenbarung unter den Voraussetzungen der §§ 72 bzw. 73 zu erreichen; erst wenn sich dieser Weg als nicht gangbar erweise, weil z. B. die notwendige richterliche Anordnung nicht vorliege (§ 73), sei der ersuchte Leistungsträger verpflichtet, die gewünschten Daten im Rahmen der Amtshilfe des § 68 zu offenbaren. Ich halte dies für eine interessante Variante. Aber auch in diesem Fall ist dann die Zulässigkeit der Offenbarung auf die in § 68 genannten Datenarten beschränkt.

Bei der Überprüfung eines Einzelfalles sind zwei weitere allgemein bedeutsame Probleme der Amtshilfe zutage getreten:

— Im Rahmen des § 68 sind u. a. Namen und Anschriften des derzeitigen Arbeitgebers des Betroffenen zu offenbaren. In dem fraglichen Einzelfall hatte ein Arbeitsamt auf Ersuchen der Polizei Namen und Anschrift desjenigen Arbeitgebers des Betroffenen offenbart, an den der Betroffene vermittelt worden war. Wie sich später herausstellte, hatte der Betroffene im Zeitpunkt der Offenbarung den Arbeitgeber gewechselt. Das Arbeitsamt hatte also die Anschrift eines früheren Arbeitgebers offenbart; dies ist jedoch (gegenüber der Polizei) nur nach Maßgabe des § 73 auf richterliche Anordnung zulässig. Daraus ergibt sich die Folgerung, daß bei der Offenbarung von Namen und Anschrift eines Arbeitgebers im Rahmen der Amtshilfe besondere Vorsicht geboten ist. Der ersuchte Leistungsträger muß sich vor einer solchen Offenbarung vergewissern, daß der ihm bekannte Arbeitgeber tatsächlich auch der derzeitige Arbeitgeber ist.

— Für die Amtshilfe ist Schriftform nicht vorgeschrieben. Offenbarungen im Rahmen der Amtshilfe können demnach auch mündlich erfolgen. Zur eigenen Sicherheit und zur Kontrollierbarkeit der geleisteten Amtshilfe sollten darüber in der Regel aber Aufzeichnungen (Aktennotizen) gemacht werden. Durch solche Aufzeichnungen in der Akte können andererseits schutzwürdige Belange des Betroffenen beeinträchtigt werden, so z. B. sind Nachteile für einen Arbeitsuchenden nicht auszuschließen, wenn dem Arbeitsvermittler ständig präsent ist, daß sich Verfassungsschutz oder Polizei für den Betroffenen interessiert haben, oder gar, wenn Akten oder andere Unterlagen, die solche Aufzeichnungen enthalten, anderen Stellen — berechtigterweise — zugänglich gemacht werden. Ich halte es deshalb für geboten, daß Schriftwechsel bzw. Aufzeichnungen über geleistete Amtshilfe gesondert verwahrt werden; in den Fallakten sollte sich dann lediglich ein Hinweis auf die Fundstelle befinden. Außerdem sollten sachgerechte Fristen für die Vernichtung bzw. Entfernung sowohl der Amtshilfeunterlagen wie auch der Aktenhinweise festgelegt werden.

2.11.3 Auskunftsverpflichtung nach § 840 ZPO und Schutz der Sozialdaten

Personenbezogene Daten (Sozialdaten) dürfen von einem Leistungsträger nur in den in §§ 67 bis 77 SGB X abschließend aufgezählten Fällen offenbart werden. Die Abgabe einer Drittschuldnererklärung nach § 840 ZPO ist dort als zulässiger Offenbarungstatbestand nicht genannt. Eine Offenbarung von Sozialdaten im Rahmen und für Zwecke des § 840 ZPO erscheint daher als unzulässig.

Im Interesse eines richtig verstandenen Gläubigerschutzes befriedigt dies nicht. Auch laufende Sozialleistungen unterliegen grundsätzlich der Pfändung. Die Leistung selbst ist also vor dem Zugriff des Gläubigers nicht geschützt, während damit zusammenhängende notwendige Informationen als Sozialgeheimnis einem strikten Offenbarungsverbot unterliegen.

Eine Lösungsmöglichkeit könnte sich aus einer teleologischen Betrachtung der Vorschriften über das Sozialgeheimnis und den Schutz der Sozialdaten ergeben:

Zweck des gesamten Regelungskomplexes war sicherzustellen, daß niemand dadurch, daß er der Sozialversicherung angehört oder sonst Ansprüche auf Sozialleistungen hat, mehr als andere Bürger der Preisgabe seiner personenbezogenen Daten ausgesetzt werden darf. Daraus erhellt, daß sich der Sozialdatenschutz auf solche Daten bezieht, die dem Leistungsträger als solchem im Zusammenhang mit einem Versicherungsverhältnis, der Erbringung von Sozialleistungen oder der Erfüllung gesetzlicher Pflichten nach dem Sozialgesetzbuch bekannt geworden sind.

Wenn dem Pfandgläubiger die Tatsache des Sozialleistungsbezuges des Schuldners und gegebenenfalls sogar die Höhe der Leistung aber bereits bekannt ist, findet insoweit eine Offenbarung von Sozialdaten nicht statt. Darüber hinausgehende Angaben, ob und welche Ansprüche andere Personen an die Leistung stellen sowie ob und wegen welcher Ansprüche die Leistung bereits für andere Gläubiger gepfändet ist (§ 840 Abs. 1 Nr. 2 und 3 ZPO), sind dem Leistungsträger nicht in den vorgenannten Zu-

sammenhängen bekannt geworden, sondern — wie jedem anderen Schuldner auch — als Schuldner einer gepfändeten Forderung. Insofern ist der Leistungsbezieher nicht mehr als andere Bürger der Preisgabe seiner persönlichen und sachlichen Verhältnisse ausgesetzt. Denn Zweck und Ziel des Sozialdatenschutzes ist nicht, den Bezieher von Sozialleistungen vor dem Zugriff seiner Gläubiger auf diese pfändbare und gepfändete Leistung zu schützen. Die Konsequenz wäre, daß die in der Drittschuldnererklärung nach § 840 ZPO von einem Leistungsträger zu machenden Angaben nicht den „eigentlichen" Sozialdaten zuzurechnen sind und deshalb auch nicht dem besonderen Schutz und dem Offenbarungsverbot des Sozialgeheimnisses unterliegen.

Aus diesen Überlegungen habe ich keine Bedenken gegen die Abgabe einer Drittschuldnererklärung in dem insoweit notwendigen Umfang durch einen meiner Kontrolle unterstehenden Leistungsträger (s. aber auch unten Nr. 2.12.3!).

2.12 Arbeitsverwaltung

2.12.1 Entwicklung der Datenverarbeitung und des Datenschutzes in der Praxis, Rechtsentwicklung

Vor allem die Arbeitsverwaltung mit ihren 146 Arbeitsämtern mit 501 Nebenstellen hat die Last der steigenden Arbeitslosenzahlen zu bewältigen. Der arbeitslose Bürger erwartet die Vermittlung einer geeigneten neuen Tätigkeit, eine pünktliche Zahlung seiner Leistungen und gerechte Behandlung. Die Arbeitsverwaltung hat diese Aufgaben mit einem Personalbestand zu bewältigen, der nur unwesentlich höher ist als vor der Wirtschaftskrise. Sie ist darauf angewiesen, die Informationstechnik zur Vereinfachung und Beschleunigung von Verwaltungsaufgaben, aber auch als Mittel einzusetzen, den Service für die Bürger zu verbessern. Auch wenn klassische Aufgaben wie Arbeitsvermittlung und Berufsberatung weiterhin überwiegend manuell bewältigt werden, so steht doch die Arbeitsverwaltung vor einer tiefgreifenden Umstellung, die nach und nach zu Automatisierungsvorhaben in allen Aufgabenbereichen führen wird. In nenne im folgenden die wichtigsten:

Automatisierung der Arbeitsvermittlung

— Halboffene Arbeitsvermittlung „Micros" (CoArb Micros)

Als Eingangsstufe zur CoArb (Computergestützte Arbeitsvermittlung) wurde „Micros", ein Verfahren der „Mikroverfilmung offener Stellen" im Rahmen der halboffenen Arbeitsvermittlung, entwickelt. Die Stellenangebote werden in den Arbeitsämtern auf OCR-Belegen erfaßt und per Post dem Zentralamt der Bundesanstalt für Arbeit übersandt. Als Ergebnis der Verarbeitung erhalten die Arbeitsberater und Hauptvermittler täglich ein aktuelles Mikrofiche mit allen Stellenangeboten des Einzugsbereiches ihres Arbeitsamtes. Dieses Fiche weist auch die jeweiligen Arbeitgeber der offenen Stellen aus. Zusätzlich wird ein weiteres Fiche für die Mikrofilmlesegeräte in den Wartezonen erstellt, an denen sich Arbeitsuchende über den Bestand an Stellenangeboten informieren. Das Verfahren heißt „halboffen", weil die Arbeitgeber dabei nicht offengelegt werden.

Der Einsatz des Verfahrens ist in einem Großversuch im Landesarbeitsamts-Bezirk Nordbayern erprobt worden und soll nach Auswertung der Versuchsergebnisse zunächst auf Südbayern und Baden-Württemberg, danach auf alle Landesarbeitsamts-Bezirke ausgedehnt werden.

Bei den Vermittlungsfachkräften wird Micros später nach und nach durch das Verfahren der computergestützten Arbeitsvermittlung im Arbeitsamt (CoArb AA, s. unten) ersetzt werden, in den Wartezonen wird es jedoch bestehen bleiben.

„CoArb Micros" soll in einigen Jahren durch Verfahren abgelöst werden, bei denen Vermittler in Hauptstellen und Arbeitsämtern nicht über Mikrofilmlesegeräte, sondern über Terminals (Bildschirme und Drucker) verfügen. Zur Realisierung dieser Automatisierungsphase werden gegenwärtig verschiedene Projekte durchgeführt, und zwar:

— Computerunterstützte Arbeitsvermittlung im Fachvermittlungsdienst (CoArb FVD)

Schon seit vielen Jahren wird die Vermittlung hochqualifizierter Arbeitskräfte (insbesondere Akademiker) durch ein automatisiertes Verfahren unterstützt. Die Verarbeitung erfolgt seit 1974 zentral im sogenannten Stapelverfahren. Dazu sind die 19 Fachvermittlungsdienste und die Zentralstelle für Arbeitsvermittlung in Frankfurt mit Datenerfassungsgeräten für die Eingabe von Stellen- und Bewerbungsangeboten ausgestattet. Die Ergebnisse des zentralen Abgleichs werden in den angeschlossenen Dienststellen ausgedruckt.

— Computergestützte Arbeitsvermittlung im Arbeitsamt („CoArb AA", gelegentlich auch Marburger Verfahren genannt)

Bei diesem Verfahren werden die Sachbearbeiter über ihre Terminals direkten und sofortigen Zugriff zu den offenen Stellen der Einzugsbereiche haben. Darüber hinaus kann der Hauptvermittler Bewerberdaten mit gespeicherten Stellenangebotsdaten im Dialog abgleichen und sich das Ergebnis auf dem Bildschirm anzeigen lassen. Außerdem können u. a. Arbeitsmarktinformationen abgerufen und Vermittlungsvorschläge ausgedruckt werden. In den Auskunfts- und Beratungsstellen ist es möglich, die Stellenangebote täglich aktuell über Bildschirm zu erfassen, gegebenenfalls zu ändern oder zu löschen.

Auch beim Verfahren „CoArb AA" kann sich der Arbeitsuchende mit Hilfe von „Micros" in den Wartezonen vorinformieren.

Das Verfahren „CoArb AA" wird stufenweise weiterentwickelt. Zur Zeit werden u. a. Pro-

gramme erstellt, um neben den Stellenangeboten auch die Bewerberangebote einzubeziehen. Damit ist die Grundlage für statistische Auswertungen aller Art gegeben.

Das Verfahren „CoArb AA" wird gegenwärtig im Arbeitsamt Marburg getestet. Dabei hat sich herausgestellt, daß die Leistungsfähigkeit der benutzten Anlage nicht ausreicht, um die Arbeitsvermittlung auch in größeren Arbeitsämtern zu unterstützen. Deshalb wird gegenwärtig in einem Pilotprojekt beim Arbeitsamt Darmstadt das Verfahren auf einer Großanlage getestet.

— Bildschirmtext (Btx)

Durch eine Beteiligung am Bildschirmtext-Feldversuch in Berlin wird erprobt, ob Bildschirmtext für die Arbeitsvermittlung von Nutzen sein kann. Bei dem Versuch sollen zunächst Daten von Bewerbern aus technischen Berufen für Btx-Benutzer abrufbar sein. Bei positivem Ausgang des Versuchs soll das Verfahren auf das gesamte Bundesgebiet ausgedehnt werden. Damit wird der Anschluß eines sogenannten „externen" Rechners erforderlich (Verbindung der Bildschirmtextzentrale der Deutschen Bundespost mit einem Rechner der Bundesanstalt für Arbeit).

Automatisierung der Berufsberatung

Aus Pressemeldungen wurde mir die Einführung eines „STEP PLUS" genannten EDV-Verfahrens im Landesarbeitsamt-Bezirk Baden-Württemberg bekannt. In einem zunächst einjährigen Versuch sollen Schüler veranlaßt werden, sich über die Berufsaussichten genauer und vielseitiger als bisher zu informieren und die eigenen Fähigkeiten und Chancen konkreter einzuschätzen. In einer ersten Phase haben deshalb etwa 100 000 Haupt- und Realschüler der jeweils vorletzten Klasse ihrer Schule ein Arbeitsheft zur Selbsterkundung und einen Fragebogen erhalten, auf dem sie ihre Erwartungen und die Selbsteinschätzung ihrer Fähigkeiten angeben können. Die Fragebögen werden an eine Privatfirma versandt, die sie mit ihrem Rechner auswertet und die Ergebnisse in einem Antwortbrief den Schülern mitteilt. Die Antwort versucht, Erwartungen, Berufswünsche und Fähigkeiten auf ihre Übereinstimmung hin zu bewerten.

Es ist noch nicht sicher, ob dieser Versuch zur allgemeinen Einführung in der Arbeitsverwaltung geeignet ist. Es wird auch gegenwärtig noch von den zuständigen Stellen der Bundesanstalt geprüft, ob das Verfahren, vor allem in seinen Details, datenschutzrechtlich unbedenklich ist.

Automatisierung des Leistungswesens

— Automatisierte Datenerfassung

Im Bereich des Landesarbeitsamtes Hessen sind nunmehr alle Dienststellen mit komfortablen Datenerfassungsgeräten ausgestattet. In diesen Arbeitsämtern werden über Bildschirmgeräte Daten erfaßt und geprüft. Die Daten werden in der Nacht von Großrechnern im Zentralamt über Telefonleitungen automatisch abgerufen.

In ca. 20 Arbeitsämtern außerhalb des Landesarbeitsamts-Bezirks Hessen sind derartige Datenerfassungsgeräte für die computergestützte Datenerfassung installiert und betriebsbereit. Mit vorbereitenden Baumaßnahmen wurde in weiteren 20 Ämtern begonnen.

— Automatisierte Leistungsempfängerdatei (LED Stufe 1—3)

Seit Mai 1981 werden im Arbeitsamt Wiesbaden für die Zahlung von Arbeitslosengeld und Arbeitslosenhilfe die vorhandenen Geräte auch für Informations- und Auskunftszwecke erprobt. Eine dezentral geführte Leistungsempfängerdatei (LED), die jeweils nachts über Postleitung vom Zentralamt auf den neuesten Stand gebracht wird, ermöglicht schnellere und aktuellere Information. Im bisherigen Verfahren werden die Leistungsempfängerdaten mikroverfilmt und den Dienststellen in Form von Mikrofiches täglich auf dem Postwege übermittelt. Nach erfolgreichem Abschluß des Modellversuchs soll das Verfahren auf alle an die dezentrale Datenverarbeitung angeschlossenen Arbeitsämter ausgedehnt werden. Wegen der hohen Zahl sowie des steigenden Informationsbedürfnisses der Leistungsempfänger erhält die Auskunftserteilung immer mehr Gewicht. Das Verfahren wird dazu beitragen, den Service der Arbeitsämter wesentlich zu verbessern.

Auf Dauer erscheint das Verfahren erweiterungsbedürftig. So gilt es z. B., die Informationslücke zwischen Antragseingang und Entscheidung über den Antrag zu schließen. Eine computerunterstützte Datenerfassung bereits bei Antragseingang und Speicherung des unerledigten Antrags u. a. für Auskunftszwecke bis zur Entscheidung könnte hier Abhilfe schaffen (= LED-Stufe 3).

Zeitkritische Arbeitsvorgänge in der Leistungsabteilung können infolge von Engpässen in den Datenstellen häufig nicht hinreichend schnell weitergeleitet werden. Durch computerunterstützte Dateneingabe direkt in der Leistungsempfänger-Bearbeitungsstelle könnten eilige Vorgänge sofort erledigt werden. Darüber hinaus würde sich die Ablauforganisation (Aktentransport, doppelte Arbeitsgänge) erheblich vereinfachen.

Praxis des Datenschutzes

Eine traditionell und manuell arbeitende Verwaltung ist anders zu beurteilen als eine Verwaltung, die sich mitten in einem Umstellungsprozeß befindet. So haben sich Konflikte, die am Anfang meiner Tätigkeit mit der Arbeitsverwaltung auszutragen waren, an Problemen entzündet, die aus heutiger Sicht eher zweitrangig sind, z. B. an der Frage, ob die Hauptarbeitsmittel der Arbeitsverwaltung wie die Vermittlungskarteien ‚Dateien' im Sinne des BDSG und demnach gem. § 13 BDSG auskunftspflichtig sind. Heute kann ich sagen, daß die Zu-

sammenarbeit mit der Arbeitsverwaltung unproblematisch ist. Die Mitarbeiter haben die Aufgabe Datenschutz weitgehend als eigene angenommen, was ihnen durch interne spezielle Datenschutzlehrgänge und Schulungen im Rahmen der Verwaltungsausbildung erleichtert wird. Nicht zuletzt sei hier ein Film über den Datenschutz erwähnt, den die Bundesanstalt für Arbeit selbst erstellt hat, um allen Mitarbeitern Probleme des BDSG und des SGB X an Beispielen aus ihrer Praxis nahezubringen. Dies ist ein Beispiel dafür, wie man mit geringem Aufwand einen großen Ertrag erreichen kann.

Die Bundesanstalt hat die Aufgabe Datenschutz in einer mich jetzt überzeugenden Form organisiert:

— Mit Wirkung vom 1. April 1980 ist der Direktor des Vorprüfungsamtes der Bundesanstalt zum Beauftragten für Datenschutz und Datensicherheit bestellt worden. So ist es möglich, das mit Revisionsaufgaben betraute Vorprüfungsamt auch für Zwecke der Kontrolle des Datenschutzes in den einzelnen Arbeitsämtern zu nutzen.

— Ein Referat der Zentralabteilung der Bundesanstalt hat die Bearbeitung „gemeinsamer Angelegenheiten des Datenschutzes" übernommen.

In meinem Dritten Tätigkeitsbericht (S. 43) habe ich mir zu dieser Organisation eine abschließende Stellungnahme vorbehalten. Nach mehrjähriger Zusammenarbeit kann ich nunmehr sagen, daß die Bundesanstalt eine praxisgerechte, ökonomisch und datenschutzrechtlich sinnvolle Lösung gefunden hat. Es hat sich nämlich herausgestellt, daß die Aufgaben, die die Vorprüfungsordnung (insbesondere DA 13.01) dem Vorprüfungsamt zuweist, praktisch zu einem erheblichen Teil identisch sind mit den Aufgaben des internen Beauftragten.

Einzig unbefriedigend bleibt, daß die Antwortzeiten auf Bürgereingaben — zuständig hierfür ist die Zentralabteilung — noch immer zu lang sind (2—3 Monate). Anscheinend lassen sich diese Zeitverluste bei einer so großen Verwaltung nicht nennenswert reduzieren.

Auch das neue SGB X (mit den entsprechenden internen Erlassen der Bundesanstalt für Arbeit) hat dazu beigetragen, eine Reihe früher strittiger Fragen zu klären. So war es nach altem Recht zweifelhaft, ob Datenabgleiche zwischen einzelnen Abteilungen der Bundesanstalt zulässig sind, eine Frage, die jetzt zu bejahen ist. Das nach § 75 SGB X geregelte Verfahren für Offenbarungen zur Forschung und Planung hat erheblich zur Rechtssicherheit beigetragen. An einem ersten Genehmigungsverfahren gemäß § 75 Abs. 2 SGB X über eine Effizienzuntersuchung der Arbeitsverwaltung habe ich bei der Vertragsgestaltung mit dem Forschungsinstitut mitgewirkt.

Der nachfolgende Fall zeigt aber, daß nicht alle Auslegungsprobleme beseitigt sind. Wegen seiner Besonderheiten dürfte dieser Fall nicht verallgemeinerungsfähig sein. Ich will aber trotzdem hierüber berichten, weil er in der bundesweiten Presseberichterstattung zu einem grundlegenden Konflikt zwischen Datenschutz und innerer Sicherheit hochstilisiert wurde:

Die Polizei fahndete aufgrund einer Strafanzeige nach einem Mann wegen des Verdachts des Handtaschenraubs an seiner Ehefrau. Aufgrund ungeklärter Umstände bekam ein Polizist davon Kenntnis, daß der unbekannt verzogene Mann beim Arbeitsamt XY Arbeitslosenunterstützung erhielt. Eine telefonische Nachfrage bei der zuständigen Sachbearbeiterin brachte hierfür die Bestätigung. Der Polizist erfuhr telefonisch von ihr auch, daß sich der Mann gerade im Amt befinde. Er bat sie daraufhin, den Mann eine Zeit lang hinzuhalten, damit er ihn festnehmen könne. Nach diesem Telefongespräch kamen der Sachbearbeiterin rechtliche Bedenken, die sie ihrem Vorgesetzten, einem Volljuristen, vortrug. Dieser entschied, daß der momentane Aufenthalt des Mannes insbesondere wegen des § 68 SGB X nicht hätte mitgeteilt werden dürfen. Er wies sie deshalb an, den Gesuchten fortzuschicken, was sie tat. Die später im Amt erschienenen Polizisten trafen ihn nicht mehr an. Der gesuchte Mann wurde einige Tage später festgenommen und ein Jahr später wegen Diebstahls zu einer Freiheitsstrafe von einem Jahr verurteilt.

Gegen den Abteilungsleiter des Arbeitsamtes wurde ein Strafverfahren eingeleitet. Er ist in erster Instanz wegen Strafvereitelung im Amt zu einer Geldstrafe von 40 Tagessätzen zu je 130 DM verurteilt worden, das Landgericht Berlin hat ihn freigesprochen (Az 64 LS 06/81). Die Staatsanwaltschaft hat Revision eingelegt.

Der Abteilungsleiter hat sich in diesem Fall in einer Eingabe an mich gewandt, die Hauptstelle der Bundesanstalt mich um eine Stellungnahme gebeten. Hierin habe ich u. a. ausgeführt, daß bei der gebotenen restriktiven Auslegung des § 68 Abs. 1 SGB X „der momentane Aufenthaltsort" kein zu offenbarendes Datum ist.

Ich möchte mich nicht in ein schwebendes Verfahren einschalten und auf weitere Rechtsausführungen verzichten. Ich möchte lediglich auf ein Grundproblem dieses Falles hinweisen. Offensichtlich gibt es noch Schwierigkeiten bei der Verständigung zwischen Behörden mit unterschiedlicher Aufgabenstellung. Der nötige Interessenausgleich darf nach dem Willen des Gesetzgebers nicht zu Lasten einer Seite gehen. Meine Ausführungen oben (Nr. 2.11.2) zum gegenseitigen Verhältnis der §§ 68 und 72 SGB X dürften zeigen, daß ich dem Anliegen der Polizei durchaus Verständnis entgegenbringe. Dieser Einzelfall ist ungeeignet, eine Front zwischen Datenschutz und Sicherheitsbedürfnis aufzubauen.

2.12.2 Kontroll- und Beratungstätigkeit

Zusammenfassender Überblick für die Jahre 1978 bis 1982

Im Jahre 1979 habe ich die Hauptstelle der Bundesanstalt für Arbeit in Nürnberg überprüft. Diese Prüfung hat sich auf die Organisation des Datenschutzes innerhalb der Arbeitsverwaltung und aus-

gewählte datenschutzrechtliche Probleme beschränkt. Die damals festgestellten erheblichen Mängel (s. 2. TB, S. 30 ff.) sind inzwischen abgestellt. Nicht Gegenstand der Prüfung war die Untersuchung der Ordnungsmäßigkeit der Datenverarbeitungsprozesse gemäß § 15 Nr. 2 BDSG.

Zusätzlich habe ich Einzeleingaben von Bürgern in insgesamt 14 Arbeitsämtern überprüft. In der überwiegenden Zahl haben sich die Befürchtungen der Bürger als unberechtigt herausgestellt, es gab also keinen Anlaß zu Beanstandungen. Eine Eingabe, die wegen des komplizierten Sachverhalts mehrere Tage zusammen mit einem Mitarbeiter des Vorprüfungsamtes der BA überprüft wurde, führte zu einer förmlichen Beanstandung (vgl. 4. TB S. 18). Mängel, die in anderen Fällen festgestellt wurden, konnten meist schon vor Ort behoben werden.

In zwei Arbeitsämtern habe ich eine mehrtägige Datenschutzgesamtprüfung vorgenommen.

2.12.3 Herausgehobene Einzelfälle und Einzelfragen

Die Anzahl der Bürgereingaben ist über die Jahre weitgehend konstant geblieben, allerdings haben sich die Schwerpunkte verschoben:

In den ersten Jahren haben Bürger hauptsächlich — und zumeist undifferenziert — Auskunft aus ihren Vermittlungsunterlagen verlangt oder unsachgemäße bzw. falsche Eintragungen in ihren Unterlagen behauptet. In der geringeren Zahl der Fälle war diese Annahme zutreffend.

Viele Bürger empfanden die Angabe des Zahlungsgrundes auf Überweisungsbelegen der Bundesanstalt (z. B. „Arbeitslosenhilfe") als Diskriminierung. Diskussionen mit den Landesdatenschutzbeauftragten und im Kreis der kommunalen Spitzenverbände haben ergeben, daß das Datum „Zahlungsgrund" vor allem aus vollstreckungsrechtlichen Gesichtspunkten erforderlich ist. Auch wenn insoweit bessere Lösungen denkbar wären, so habe ich doch meine anfänglichen Bedenken zurückgestellt.

Gegenwärtig sind die Bürger, die sich an mich wenden, vor allem an der Klärung folgender Probleme interessiert:

— Das Verhältnis der Auskunftsvorschriften in § 25 SGB X und § 13 BDSG zueinander ist offensichtlich häufig noch unklar.

  In einem besonders datenschutzfreundlichen Runderlaß (Nr. 70/81 v. 18. Mai 1981) hat die Bundesanstalt die Auskunft gemäß § 13 BDSG geregelt. In diesem Erlaß wird u. a. angeordnet, Auskünfte nicht auf in Dateien gespeicherte Daten zu beschränken und sie gebührenfrei zu erteilen. Trotzdem kommt es bei einzelnen Arbeitsämtern immer wieder vor, daß die Auskunft von einer Gebühr abhängig gemacht wird. Unklarheiten bestehen in der Praxis vor allem dann, wenn die Bürger Einsicht in ihre ärztlichen/psychologischen Unterlagen nehmen und Kopien erhalten wollen. Der Wunsch nach Kopien ist mehrfach unter Hinweis auf § 13 BDSG verweigert worden, ohne daß die Voraussetzungen des § 25 SGB X geprüft wurden: Nach § 13 BDSG liegt die Ausfertigung im pflichtgemäßen Ermessen der Arbeitsämter, nach § 25 SGB X jedoch muß die Verwaltung eine Ablichtung erteilen, falls der Betroffene ein rechtliches Interesse geltend macht und die übrigen Ausschlußgründe nicht gegeben sind.

  Die Arbeitsverwaltung bereitet gegenwärtig einen neuen Runderlaß vor, der diese praktischen Unsicherheiten beseitigen soll. Diese Neufassung bereitet Schwierigkeiten, weil nach Auskunft der Bundesanstalt manche Arbeitgeber sich diese Rechtslage in der Weise zunutze machen, daß sie ihre künftigen Arbeitnehmer zur Vorlage der arbeitsamtsinernen ärztlichen und psychologischen Gutachten zwingen. Ich habe empfohlen zu prüfen, ob dieser Mißbrauch der Auskunftsrechte durch eine Regelung etwa entsprechend § 28 Bundeszentralregistergesetz verhindert werden kann.

— Nicht sehr häufig, aber regelmäßig wenden sich Gläubiger an mich, die die Arbeitsverwaltung zur Offenbarung von Sozialdaten zwingen wollen, die sie zur Geltendmachung von zivilrechtlichen Ansprüchen benötigen. Insbesondere die folgende Eingabe zeigt mir, daß der Sinn der Offenbarungstatbestände der §§ 67 ff. SGB X häufig nicht verstanden wird: Eine Steuerberatungsgesellschaft hatte zwei Arbeitsämter der gleichen Stadt um die Mitteilung gebeten, ob ein bestimmter Bürger dort Leistungen bezieht. Dem Schreiben lag ein Vollstreckungsbefehl bei. Das Arbeitsamt I hat die gewünschte Auskunft erteilt, das Arbeitsamt II sie zutreffend verweigert, weil die §§ 67 ff. keine Offenbarung zulassen. Es war der Steuerberatungsgesellschaft — begreiflicherweise — nur schwer zu vermitteln, daß es nur in wenigen präzis geregelten Fällen Aufgabe der Sozialleistungsträger ist, bei der Durchsetzung privatrechtlicher Ansprüche zu helfen (s. aber auch oben Nr. 2.11.3).

— Aus einer Vielzahl gleichartiger Eingaben weiß ich, daß das Verfahren der Gewährung von Arbeitslosenhilfe unbefriedigend ist. Das Arbeitsamt läßt sich gegenwärtig die erforderlichen Einkommensbescheinigungen unterhaltspflichtiger Angehöriger über den Arbeitslosen vorlegen. Der Arbeitslose erhält so Kenntnis der Einkommensverhältnisse seines Angehörigen, zumeist des Vaters. Allen Eingaben lagen problematische Familienverhältnisse, zumeist Vater-Sohn-Konflikte, zugrunde. Das gegenwärtige Verfahren verschärft diese Familienkonflikte offensichtlich noch.

  Mehrfache und langwierige Bemühungen, die Arbeitsverwaltung zu einer Verfahrensumstellung zu bewegen, sind bisher gescheitert. Im Interesse der Betroffenen appelliere ich an die Arbeitsverwaltung, das Arbeitslosenhilfe-Verfahren insoweit umzustellen.

2.12.4 Ausblick

Die erwähnten Umstellungsprozesse in der Arbeitsverwaltung bringen eine Vielzahl neuartiger Daten-

schutzprobleme, vor allem ungeklärter technisch-organisatorischer Probleme mit sich. Ich habe die Arbeitsverwaltung mehrfach bei Pilotprojekten aus den Bereichen Arbeitsvermittlung und Leistungswesen beraten, allerdings lagen die entsprechenden Aktivitäten ehe am Rande meiner Prioritäten. Dies wird sich in Zukunft ändern müssen, zumal ich gebeten wurde, schon bei der Entwicklung neuer Systeme beratend Datenschutzanregungen einzubringen. In der Vergangenheit betraf diese Beratungstätigkeit sowohl Fragen der Hardware-Sicherheit — auf Einzelheiten möchte ich hier verzichten, um nicht ungerechtfertigterweise einen einzigen Hersteller zu kritisieren — als auch Gedankenmodelle zum Datenschutz im „papierlosen Büro" der Zukunft.

Ein weiterer Schwerpunkt für die Zukunft wird es sein, den gesamten Bereich des Umgangs mit ärztlichen und psychologischen Gutachten neu und umfassend zu regeln.

2.13 Rentenversicherung

2.13.1 Entwicklung der Datenverarbeitung und des Datenschutzes in der Praxis; Rechtsentwicklung

Im Bereich Rentenversicherung bin ich nur für den kleineren Teil der Versicherungsträger zuständig; die überwiegende Zahl der Träger befindet sich im Zuständigkeitsbereich der Landesbeauftragten für den Datenschutz bzw. der Datenschutzkommission Rheinland-Pfalz.

Mit dem Verband Deutscher Rentenversicherungsträger (VDR), der Bundesversicherungsanstalt für Angestellte (BfA) und anderen Trägern hat es während meiner Amtszeit eine Vielzahl von Arbeitskontakten gegeben. Ich habe eine Reihe von Kontrollen gemäß § 19 Abs. 1 BDSG durchgeführt.

Aus diesen Kontrollen hat sich in allen Fällen eine gute Zusammenarbeit entwickelt. Die Versicherungsträger haben schon seit langer Zeit dem Schutz von Sozialdaten gegenüber Stellen außerhalb der Sozialversicherung große Bedeutung zugemessen. Andererseits verstellt die Beibehaltung einer bestimmten Praxis manchmal den Blick für neue Entwicklungen. Die Rentenversicherungsträger haben daher meine Kontrolle begrüßt.

Besonders in der Rentenversicherung ist in den letzten Jahren eine grundlegende technologische Umgestaltung zu verzeichnen: Neben der Weiterführung der bestehenden zentralen Anwendungen wird das Bild vom zunehmenden Einsatz sogenannter Dialogsysteme bestimmt: Der Sachbarbeiter erfüllt seine Aufgabe im unmittelbaren Dialog mit Computersystemen. Die technische Realisierung solcher Systeme besteht einmal im Einsatz von Geräten der mittleren Datentechnik, zum anderen im Einsatz von Terminals, die mit einem zentralen Rechner verbunden sind.

Im Verlauf einer derartigen Umstellung entstehen eine Vielzahl juristischer, organisatorischer und technischer Fragen. Diese erstrecken sich von der Erforderlichkeit von Daten oder gar ganzer Verfahren bis zur Realisierung technischer und organisatorischer Maßnahmen wie z. B. Zugriffskontrolle oder Eingabekontrolle.

Bei der Lösung solcher Probleme hat sich meine Beratung — auch aufgrund der bei anderen Stellen gewonnenen Erfahrungen — in vielen Fällen als durchaus hilfreich erwiesen und wurde gerne angenommen.

Dies gilt auch für die organisatorische Einbettung des Datenschutzes bei den Rentenversicherungsträgern. Dabei war sicherzustellen, daß die Anliegen des Datenschutzes bei der Entwicklung neuer DV-Systeme sowie bei konventionellen Verwaltungsabläufen in ausreichendem Maße berücksichtigt werden. Hier konnten gemeinsam mit den Rentenversicherungsträgern Modelle zur Beteiligung der internen Datenschutzbeauftragten entwickelt werden.

Aus der Entwicklung des Datenschutzrechts haben sich zusätzliche Datenschutzprobleme nicht ergeben.

2.13.2 Kontroll- und Beratungstätigkeit

Bundesversicherungsanstalt für Angestellte (BfA)

Der Entwicklung des Datenschutzes bei der BfA habe ich wegen der Größe und Bedeutung dieses Versicherungsträgers besondere Aufmerksamkeit gewidmet. In einer zweiwöchigen Kontrolle im Jahre 1981 und einer Vielzahl von Gesprächen sowie aus zahlreichen Stellungnahmen zu Anfragen meines Amtes habe ich folgenden Gesamteindruck gewonnen:

Der interne Datenschutzbeauftragte hat hervorragende Arbeit geleistet. Er hat sich bemüht, Datenschutzaspekte bereits bei der Entwicklung von DV-Systemen einzubringen, hat durch Schulung der Mitarbeiter der BfA dazu beigetragen, den Datenschutzgedanken auch in der täglichen Praxis wirksam werden zu lassen und hat für Stellungnahmen sorgfältig recherchiert.

Leider gibt es nach meiner Erfahrung jedoch in den Fachabteilungen noch immer Mitarbeiter, die die Bedeutung des Sozialdatenschutzes offenbar unterschätzen. So geschieht es gelegentlich, daß Versicherte, die sich mit Fragen oder Beschwerden dorthin wenden, Antworten erhalten, die wenig datenschutzfreundlich, wenig versichertenfreundlich sind. Oft wird zu formal argumentiert, die Bearbeitung dauert zu lange. Dies ändert sich erst dann, wenn von mir der interne Datenschutzbeauftragte der BfA eingeschaltet wird. So schreibt mir ein Petent: „Meine Kritik am Verhalten der BfA und mein Verdacht auf Datenmißbrauch sind ... ausgeräumt. Eine Beantwortung meiner Schreiben an die BfA in angemessener Frist hätte meine Beschwerde an Sie überflüssig gemacht." Ich gehe davon aus, daß es der BfA gelingen wird, solche Bearbeitungsprobleme künftig zu vermeiden.

Meine im Vierten Tätigkeitsbericht (S. 13f.) geschilderten Kontrollergebnisse und Vorschläge haben in der BfA eine Reihe von Untersuchungen und Maßnahmen ausgelöst:

— Die im Hinblick auf Lesbarkeit und Transparenz der Übersicht gemäß § 15 Abs. 2 BDSG festgestellten Mängel wurden inzwischen behoben.

— Die BfA hat zugesagt, die von mir geforderte EDV-Revision zu schaffen. Hierdurch soll sichergestellt werden, daß Datenschutzaspekte bereits bei der Entwicklung von Systemen ausreichend berücksichtigt werden.

— Als technisch-organisatorischen Mangel hatte ich die unzureichende Sicherung des Umlaufs und der Verwaltung der Versichertenakten bezeichnet. Ich hatte die BfA aufgefordert, nach Möglichkeiten zu suchen, diese Mängel abzustellen, ohne Bürgernähe und Qualität der Beratungstätigkeit der BfA zu beeinträchtigen.

  Eine Analyse der einzelnen Gefahrenpunkte durch die BfA und die Gegenüberstellung des jeweiligen Aufwandes haben ergeben, daß eine wesentliche Verbesserung der Sicherheit nur erreicht werden kann, wenn es gelingt, den Zugang der Besucher auf die für sie vorgesehenen Bereiche (Auskunfts- und Beratungsstelle) zu beschränken. Daraufhin hat die BfA bauliche, technische und organisatorische Maßnahmen zur Abgrenzung dieser Bereiche von den anderen Diensträumen bzw. Gebäudeteilen eingeleitet.

— Ein Arbeitsschwerpunkt meiner Kontrolle war das Rehabilitations-Gesamtsystem. Es handelt sich um ein automatisiertes Verfahren, das die Sachbearbeitung und die ärztliche Begutachtung von Rehabilitationsleistungen unterstützen und steuern soll.

  Ich habe in meinem Vierten Tätigkeitsbericht (S. 13f.) einige klärungsbedürftige Probleme genannt, z. B. die Trennung von Verwaltungsdaten und medizinischen Daten in der Sachbearbeitung. Diese Frage wurde von der BfA untersucht und mit anderen Rentenversicherungsträgern besprochen. Die Untersuchung hat ergeben, daß die von mir vorgeschlagene Trennung der Daten aus der Sicht der BfA nicht durchgeführt werden kann. Zwar wurde eingeräumt, daß eine solche Maßnahme sicherlich zum größeren Schutz der Betroffenen beitragen würde. Gegen eine Realisierung in der Praxis sprechen jedoch sowohl aus ärztlicher als auch aus verwaltungsmäßiger Sicht eine Reihe von Gründen, die hier nicht im einzelnen ausgeführt werden müssen. Als Beispiel mag das Argument der BfA stehen, daß die Trennung der Daten in Verbindung mit einer getrennten Aktenführung dazu führen würde, daß der Verwaltung eine eigenverantwortliche Entscheidung sehr erschwert, wenn nicht gar unmöglich gemacht würde. Das Untersuchungsergebnis der BfA habe ich zunächst akzeptiert. Da ich aber dem Problem grundsätzlich Bedeutung zumesse, werde ich weiterhin mit der BfA und anderen Versicherungsträgern nach Alternativen suchen.

— Bei der Datenfernübertragung der BfA halte ich insbesondere wegen der geographischen Lage Berlins eine kryptographische Verschlüsselung der Datei für unerläßlich. Die BfA hat dies zugesagt.

— Das Zugangskontrollsystem der BfA sowie die Registrierung von Ferngesprächen bleiben weiter zu beobachten. Beide Verfahren wie auch das Erstellen sogenannter „Leistungsstatistiken" bei Bildschirmarbeitsplätzen bergen die Gefahr einer zu weitgehenden Leistungs- und Verhaltenskontrolle der Mitarbeiter in sich. Auf dieses Problem ist allgemein im Abschnitt 2.4.3 eingegangen worden.

Eine Reihe von Mitarbeitern der BfA hat sich an mich gewandt wegen der „Prüfung des Datenverarbeitungspersonals der BfA durch den Verfassungsschutz".

Das Rechenzentrum der BfA wurde durch einen Erlaß des BMA zum sicherheitsempfindlichen Bereich erklärt. Dies hat zur Folge, daß nicht nur alle dort tätigen Mitarbeiter sicherheitsüberprüft werden, sondern auch andere Mitarbeiter des Datenverarbeitungsbereichs. Von dieser Sicherheitsüberprüfung sind ca. 300 Mitarbeiter der BfA und darüber hinaus eine Reihe von Mitarbeitern solcher Firmen betroffen, die Software im Auftrag der BfA entwickeln. Über 50 dieser Beschäftigten halten dies für unangemessen und haben sich deshalb mit Eingaben an mich gewandt.

Auch ich habe erhebliche Zweifel, ob eine Sicherheitsüberprüfung in diesem Umfang erforderlich ist. Zwar bestreite ich nicht, daß bei der BfA hochsensible Daten gespeichert sind. Ich bin auch der Meinung, daß die Mitarbeiter, die Zugang zu diesen Daten haben, sorgfältig ausgewählt werden müssen. Der Sicherheitsbereich ist jedoch möglicherweise falsch zugeschnitten.

Ich werde mit dem BMA und der BfA weitere Gespräche zur Klärung dieser Fragen führen. Ich halte es für sinnvoll, in jedem Einzelfall zu entscheiden, ob eine Sicherheitsüberprüfung erforderlich ist. Die gewissermaßen „automatische" Überprüfung aller Mitarbeiter eines Funktionsbereichs erscheint unangemessen.

Insgesamt bleibt festzuhalten, daß die BfA sich bereit gezeigt hat, die Mehrzahl meiner Anregungen zu realisieren. Auch viele der von Petenten vorgebrachten Probleme konnten zufriedenstellend gelöst werden.

Verband Deutscher Rentenversicherungsträger (VDR)

Bei der Kontrolle des VDR habe ich festgestellt, daß dieser bei seinem Bemühen um mehr Datensicherheit zwar beachtliche Erfolge zu verzeichnen hatte, daß aber weitere Maßnahmen erforderlich waren, die umfangreichen Datensammlungen des Verbandes ausreichend zu schützen. Ich habe den VDR deshalb aufgefordert,

— auf der Basis einer verbesserten Übersicht nach § 15 Nr. 1 BDSG eine Risiko- und Schwachstellen-

analyse durchzuführen, die das Entwickeln eines Gesamtsystems ermöglicht,

— die Transparenz hinsichtlich der Zuständigkeit und Verantwortlichkeit der fünf Abteilungen des Verbandes zu verbessern,

— sicherzustellen, daß beim VDR nur solche Datenverarbeitungsaufgaben durchgeführt werden, die sich auf die gesetzlich festgelegten Aufgaben beschränken,

— Umfang und Inhalt der vorhandenen Datensammlungen auf ihre Erforderlichkeit zu überprüfen.

Die Auseinandersetzungen mit dem Verband zu diesen Problemen zogen sich über einen längeren Zeitraum hin. Schließlich konnten die bestehenden Meinungsverschiedenheiten in mehreren Gesprächen beigelegt werden. Einvernehmlich wurden folgende Ergebnisse erzielt:

— Die Übersicht nach § 15 Nr. 1 BDSG wurde verbessert, eine Risiko- und Schwachstellenanalyse wurde durchgeführt. Dabei erkannte Mängel wurden abgestellt; z. B. wurde die Zugangskontrolle verbessert.

— Die organisatorische Transparenz des Verbandes wurde verbessert. Mir war besonders an einer klaren organisatorischen Abgrenzung der Datenstelle der Deutschen Rentenversicherung (§ 14 Abs. 1 2. DEVO) von den übrigen Aufgaben gelegen.

— Die Überprüfung von Umfang und Inhalt der vorhandenen Datensammlungen auf ihre Erforderlichkeit hat zu einer Reduzierung geführt:

  Bereits vor der eigentlichen Kontrolle waren in der Stammsatzdatei (etwa 45 Mio. Sätze) die Anschriften der Versicherten durch Anschriftenvergleichszahlen ersetzt worden.

— Das wichtigste und weit über diesen konkreten Anlaß hinaus wirkende Ergebnis war, daß die sogenannte DEVO/DÜVO-Sicherungsdatei mit bis zu 75 Millionen personenbezogenen Datensätzen bis Ende 1981 eingestellt werden konnte. Ich halte diese Maßnahme deshalb für so wichtig, weil es hier gelungen ist, das hohe Risiko derart umfangreicher, zentral geführter Datensammlungen deutlich zu machen. Aus diesem Grunde war an die Erforderlichkeitsprüfung ein strenger Maßstab anzulegen.

2.14 Krankenversicherung

2.14.1 Entwicklung der Datenverarbeitung und des Datenschutzes in der Praxis; Rechtsentwicklung

Meine Zuständigkeit im Bereich der Krankenversicherung erstreckt sich auf die bundesunmittelbaren Krankenkassen — das sind die meisten Ersatzkassen für Arbeiter und für Angestellte —, die Ortskrankenkasse Bremerhaven und Wesermünde, die knappschaftliche Krankenversicherung und eine große Zahl von Betriebskrankenkassen. Innerhalb dieses Zuständigkeitsbereichs wurde eine Reihe von Kontrollen gemäß § 19 Abs. 1 BDSG durchgeführt. Hinsichtlich der technischen Entwicklung ergab sich ein ähnliches Bild wie in der Rentenversicherung: Alle besuchten Kassen sind inzwischen zur Dialogverarbeitung übergegangen bzw. sind dabei, entsprechende Systeme zu entwickeln. Dabei werden entweder Anlagen der mittleren Datentechnik eingesetzt oder Terminals mit Verbindung zu großen Systemen benutzt.

Die Beratungsgespräche mit den Entwicklern der Systeme (z. B. mit Vertretern des Bundesverbandes der Ortskrankenkassen) haben meist zu einem Einvernehmen geführt. Besondere Probleme zeigten sich bei der Datensicherung. Insbesondere für die großen Ersatzkassen mit ihren zahlreichen Geschäftsstellen, die oft in angemieteten Räumen untergebracht sind, war es schwierig, angemessene Sicherungsmaßnahmen zu treffen. Bei der Bewertung der Risiken und ihrer angemessenen Abwehr haben insbesondere die internen Datenschutzbeauftragten der Kassen eine umfangreiche Arbeit bewältigt.

Spezifische Probleme gab es bei Betriebskrankenkassen bezüglich der Verbindung zum Arbeitgeber. Darauf wird im folgenden noch eingegangen.

Insgesamt ist mein Eindruck vom Stand des Datenschutzes bei den besuchten Krankenkassen positiv. Dies trifft — von Ausnahmen abgesehen — vor allem für den Schutz der Sozialdaten gegenüber Stellen außerhalb des Sozialversicherungsbereichs zu. Intern gibt es bei einigen Kassen noch Probleme. Beispielsweise war bei Kontrollen und aus Eingaben von Betroffenen festzustellen, daß der Umgang mit Diagnosedaten *der Mitarbeiter* von Krankenkassen des öfteren noch Mängel aufweist (vgl. unten Nr. 2.14.4).

Das Recht der gesetzlichen Krankenversicherung war in den letzten fünf Jahren zahlreichen strukturellen und kostenwirksamen Änderungen unterworfen. Manche neuen Bestimmungen gaben Veranlassung zu neuen Überlegungen und Beurteilungen möglicher datenschutzrechtlicher oder datenschutzpraktischer Auswirkungen und etwa notwendiger Konsequenzen.

— Als Folge der Neuregelung der Beitragspflicht der Rentner ab 1. Januar 1983 ist die Höhe der gesetzlichen Rente und sonstiger Versorgungsbezüge sowie des Arbeitseinkommens des Rentners durch die Krankenkasse zu ermitteln und zu erfassen. Die Krankenkasse wiederum hat in den zutreffenden Fällen der Zahlstelle der Versorgungsbezüge den auf diese Bezüge entfallenden Beitragsanteil mitzuteilen (zu offenbaren). Daraus kann die Zahlstelle — bei Betriebsrenten u. ä. ist dies z. B. der frühere Arbeitgeber des Rentners — durch einfache Rückrechnung die Höhe der gesetzlichen Rente und eventuell anderer Einkommen ermitteln. Letzteres hat auch schon zu Protesten in Einzeleingaben geführt, die ich jedoch nur mit dem Hinweis auf die gesetzliche Regelung beantworten konnte. In einem Einzelfall hat die zuständige Krankenkasse

das Problem dadurch gelöst, daß sie den betroffenen Rentner als „Selbstzahler" behandelt. In diesem Fall braucht der Zahlstelle der auf die Versorgungsbezüge entfallende Beitragsanteil nicht mitgeteilt zu werden und die unerwünschte Errechnung des sonstigen Einkommens des Rentners durch seinen früheren Arbeitgeber ist unmöglich.

— Das Krankenversicherungs-Kostendämpfungsgesetz vom 27. Juni 1977 hat in das Zweite Buch der RVO zwei in datenschutzrechtlicher Hinsicht besonders bedeutsame Vorschriften eingefügt:

  Die Krankenkasse kann die Krankheitsfälle vor allem im Hinblick auf die in Anspruch genommenen Leistungen überprüfen und den Versicherten und den behandelnden Arzt über die in Anspruch genommenen Leistungen und ihre Kosten unterrichten (§ 223 RVO). Dafür ist Voraussetzung, daß die Leistungen und Kosten möglichst umfassend personenbezogen, d. h. auf den Versicherten und auf den Arzt bezogen, erfaßt und gespeichert werden; dies war bis zum Inkrafttreten dieser Vorschrift weder erforderlich, noch geschah und geschieht dies so in der bisherigen Praxis.

  Die Grundlage für diese umfassende Datenerfassung und Datenspeicherung soll das in § 319 a RVO vorgeschriebene Mitgliederverzeichnis bieten, in das die Aufzeichnungen aufzunehmen sind, die zur rechtmäßigen Erfüllung der Aufgaben der Krankenkassen erforderlich sind. Inhalt und Form des Mitgliederverzeichnisses bestimmt der Bundesminister für Arbeit und Sozialordnung durch Rechtsverordnung. Darauf werde ich unter Abschnitt 2.14.5 noch näher eingehen.

— Ebenfalls auf Leistungs- und Kostentransparenz sowie auf Kostensenkung zielt die durch das Krankenhaus-Kostendämpfungsgesetz vom 22. Dezember 1981 geschaffene Errichtung von Prüfungsausschüssen zur Überwachung der Wirtschaftlichkeit der Krankenhauspflege (§ 373 RVO). Die Krankenhäuser und die Krankenhausärzte sind nach dieser Vorschrift verpflichtet, dem Prüfungsausschuß die für die Wahrnehmung seiner Aufgaben notwendigen Unterlagen vorzulegen und Auskünfte zu erteilen. Praktische Erfahrungen mit der Tätigkeit der Prüfungsausschüsse liegen mir noch nicht vor. Es wird aber darauf zu achten sein, daß hier nicht unbefugt und unnötig ärztliche Geheimnisse offenbart werden.

2.14.2 Zusammenfassender Überblick über die Jahre 1978 bis 1982

Seit der Aufnahme meiner Tätigkeit habe ich bei neun verschiedenen Krankenkassen mehr oder weniger umfangreiche Kontrollen durchgeführt, und zwar bei fünf Ersatzkassen, zwei Betriebskrankenkassen, der Bundesknappschaft und bei der Ortskrankenkasse Bremerhaven und Wesermünde.

Bewußte Verstöße gegen Datenschutzvorschriften und mißbräuchliche Verwendungen der gespeicherten Daten der Versicherten habe ich bei den kontrollierten Kassen nicht festgestellt. Mehrfach waren jedoch Mängel im organisatorischen und sicherungstechnischen Bereich festzustellen, aufgrund derer die Möglichkeit von Mißbräuchen nicht auszuschließen war, die dann von den Verantwortlichen nur schwer zu entdecken oder nachzuweisen gewesen wären. In diesem Zusammenhang sind zu nennen:

— fehlende oder mangelhafte Übersicht über die Art der gespeicherten Daten (§ 15 Nr. 1 BDSG); eine vollständig und richtig geführte Übersicht ist eine wesentliche Voraussetzung für die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme (§ 15 Nr. 1 BDSG),

— unzureichende Sicherung des Rechenzentrums, des Bandarchivs oder der manuell geführten Leistungskarten, die in einigen Fällen in nicht verschließbaren Schränken gelagert waren.

Trotz solcher Mängel war im Bereich der automatisierten Datenverarbeitung meist ein ausgeprägtes Datenschutzbewußtsein vorhanden. Weniger ausgeprägt war es — jedenfalls in der Anfangszeit — im Bereich der manuellen Datenverarbeitung. So war bei einigen Kassen nicht erkannt worden, daß auch manuell geführte Karteien, z. B. die Leistungskartei, den Begriff einer Datei im Sinne des § 2 Abs. 3 Nr. 3 BDSG erfüllen und damit den Vorschriften des BDSG unterliegen. Dies führte zu der irrigen Annahme, die auf solchen Karten enthaltenen personenbezogenen Daten unterlägen nicht der Auskunftspflicht nach § 13 Abs. 1 BDSG. Bei einer Kasse wurde auf Verlangen des Betroffenen zwar Auskunft über die auf der Vorderseite der Karte enthaltenen Leistungsdaten, nicht aber über die Diagnosedaten auf der Rückseite erteilt.

Weitere Schwierigkeiten bereitet offensichtlich immer noch die Umsetzung der Vorschrift des § 9 Abs. 2 BDSG. So werden leider auch heute noch — fast fünf Jahre nach Inkrafttreten dieser Vorschrift — Daten beim Betroffenen mit Formularen erhoben, die den vorgeschriebenen Hinweis auf die Rechtsgrundlage der Datenerhebung bzw. auf die Freiwilligkeit der Angaben nicht oder nicht in der Form enthalten, die es dem Betroffenen ermöglicht, kritisch zu prüfen, ob er zu den verlangten Angaben verpflichtet ist und für welche Aufgaben diese Angaben erforderlich sind.

Über weitere Einzelheiten bisheriger Kontrollen habe ich in den vorausgegangenen Tätigkeitsberichten informiert (1. TB S. 35, 2. TB S. 34, 3. TB S. 40).

2.14.3 Auftragsdatenverarbeitung

— Viele, vor allem kleinere Kassen lassen die automatisierte Verarbeitung ihrer Daten bei einem gemeinsamen Rechenzentrum, z. B. ihres Landesverbandes, durchführen. Nach den Vorschriften des BDSG und des SGB X über die Auftrags-

datenverarbeitung bleibt der Auftraggeber, also die jeweilige Krankenkasse, speichernde Stelle und damit „Herr der Daten“ (§ 8 Abs. 1 BDSG, § 80 SGB X). Dies hat zur Folge, daß die Verantwortung für die Einhaltung der Datenschutzvorschriften weiterhin beim Auftraggeber liegt und nicht etwa auf den Auftragnehmer übergeht. Es zeugt von einem falschen Rechtsverständnis, wenn der Vorstand einer Krankenkasse mir auf diesbezügliche Hinweise schriftlich mitteilt, er gehe davon aus, daß der Auftragnehmer die Vorschriften des Datenschutzes beachte; nach seiner Auffassung könne das Gesetz wohl nicht so interpretiert werden, daß alle angeschlossenen Krankenkassen die Einhaltung datenschutzrechtlicher Vorschriften in dem gemeinsamen Rechenzentrum prüfen.

Genau dies sieht das Gesetz jedoch vor: Nach § 15 BDSG hat die speichernde Stelle — dies ist der Auftraggeber — die Ausführung des Bundesdatenschutzgesetzes und anderer Rechtsvorschriften über den Datenschutz sicherzustellen und insbesondere dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme überwacht wird. Sie hat erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen (§ 80 Abs. 2 SGB X). In welcher Form diese Verpflichtungen erfüllt werden, z. B. durch einen Beauftragten für alle Mitgliedskassen, bleibt dem Auftraggeber weitgehend überlassen.

2.14.4 Mitarbeiterdaten

Mitarbeiter in den Krankenkassen sind in der Regel auch bei dieser Kasse krankenversichert. Werden die versicherten Mitarbeiter im allgemeinen Mitgliederbestand geführt und in der allgemeinen Leistungsabteilung betreut, so gelangen alle versicherungsrechtlichen und leistungsrelevanten Daten einschließlich von Gesundheitsdaten dieses Mitarbeiters nicht nur dem zuständigen Kollegen in der Krankenversicherung, sondern häufig auch einem Vorgesetzten zur Kenntnis, der gleichzeitig Fachvorgesetzter und mit Personalführungsaufgaben betraut ist. Mehrere Eingaben haben mir gezeigt, daß diese Praxis für manche Betroffene ein schwerwiegendes Problem darstellt.

Es ist allgemein anerkannt, daß der Arbeitgeber medizinische Daten (Diagnosen u. a.) der bei ihm Beschäftigten nicht erhalten darf. Dies muß auch dann gelten, wenn die Krankenkasse (die diese Daten für ihre Aufgaben braucht) gleichzeitig Arbeitgeber ist. Daraus ergibt sich nach meiner Auffassung die Notwendigkeit einer möglichst vollständigen Trennung der Funktionsbereiche „Krankenkassen“ und „Personalverwaltung“. Dieses Problem wurde bei verschiedenen Krankenkassen, abhängig auch von der jeweiligen Größe der Kasse (mehrere Geschäftsstellen) unterschiedlich gut — oder auch überhaupt nicht — gelöst.

Bei der Bundesknappschaft mit ihren zahlreichen Geschäftsstellen werden die Aufgaben der Krankenversicherung für die Mitarbeiter nicht bei den Geschäftsstellen („Krankenkassen“), sondern in einer eigenen Organisationseinheit der Hauptverwaltung durchgeführt. Diese Lösung sollte als Vorbild für andere Kassen dienen. Wo dies — etwa wegen zu geringer Größe — nicht möglich ist, muß nach anderen Lösungen gesucht werden.

Ein spezifisches Datenschutzproblem ergab sich bei Betriebskrankenkassen:

Bei den Betriebskrankenkassen gehören den Selbstverwaltungsorganen (Vertreterversammlung, Vorstand) außer den Vertretern der Versicherten auch der Arbeitgeber oder sein Vertreter an. Dem Arbeitgeber als Mitglied eines Selbstverwaltungsorgans oder seinem Vertreter (in einem konkreten Fall war der Vertreter Vorsitzender des Vorstandes der Kasse und zugleich Personalchef des Unternehmens) können personenbezogene Daten aus dem Bereich der Krankenkasse zur Kenntnis gelangen, die ihm als Arbeitgeber bzw. Personalchef nach den Vorschriften über den Schutz der Sozialdaten nicht offenbart werden dürften. Dies gilt z. B. für Diagnoseangaben bei Arbeitsunfähigkeit von Beschäftigten.

Ich habe die Problematik an den Bundesminister für Arbeit und Sozialordnung herangetragen und mit ihm Lösungsmöglichkeiten in einer gemeinsamen Besprechung erörtert. Das Ergebnis fand seinen Niederschlag in einem Rundschreiben des Bundesverbandes der Betriebskrankenkassen an seine Mitgliedskassen vom 7. Dezember 1982. Darin wird mit erfreulicher Entschiedenheit darauf hingewiesen, daß aufgrund der gesetzlichen Zuständigkeitsverteilung zwischen Vorstand und Geschäftsführung einer Krankenkasse personenbezogene Daten, insbesondere solche medizinischer Art, vom Geschäftsführer in der Regel nicht an den Vorstand oder einzelne Vorstandsmitglieder übermittelt werden dürfen, weil der Vorstand diese Daten im Rahmen der Wahrnehmung von Aufgaben der Krankenkasse regelmäßig nicht benötigt. Ergänzend ist festzuhalten, daß in unumgänglichen Ausnahmefällen — entsprechend der Absprache — für eine Übermittlung personenbezogener Daten an die Selbstverwaltungsorgane oder an einzelne ihrer Mitglieder die Einwilligung der Betroffenen eingeholt werden muß.

2.14.5 Mitgliederverzeichnis nach § 319 a RVO

Anfang des vergangenen Jahres bin ich von verschiedenen Seiten darauf aufmerksam gemacht worden, daß im Bundesarbeitsministerium Vorbereitungen zum Erlaß der in § 319 a RVO vorgesehenen Rechtsverordnung über Inhalt und Form des von den Krankenkassen zu führenden Mitgliederverzeichnisses laufen (vgl. auch oben 2.14.1); gleichzeitig wurde mir ein Katalog mit über 200 Datenarten übermittelt, deren Aufnahme in das Mitgliederverzeichnis vom BMA zur Diskussion gestellt worden war. Die mir zugegangenen Hinweise habe ich zum Anlaß genommen, den BMA, der mich über das laufende Vorhaben nicht informiert hatte, um Beteiligung zu bitten und meine datenschutzrechtliche

Beratung anzubieten. Meine vorläufige Einschätzung, die ich dem BMA dabei mitgeteilt habe, stellt sich wie folgt dar:

Die in engem Zusammenhang stehenden Vorschriften der §§ 223 und 319 a RVO waren bereits während der parlamentarischen Beratungen umstritten. So hatte sich z. B. der Verband der Angestellten-Krankenkassen dahin gehend geäußert, daß kein Bedürfnis bestehe, den Krankenkassen von Gesetzes wegen die Führung von Mitgliederverzeichnissen vorzuschreiben, mit denen eine totale Erfassung aller personenbezogenen Daten des einzelnen Versicherten ermöglicht werde. Es würde auf diese Weise ein Instrument geschaffen werden, das eine umfassende Durchleuchtung der persönlichen Verhältnisse der Versicherten nach sich ziehe und eine bedenkliche Gefährdung des Anspruchs auf Schutz des allgemeinen Persönlichkeitsrechts mit sich bringe. Darüber hinaus müßten verwaltungstechnische Voraussetzungen geschaffen werden, die mit erheblichen Kosten verbunden seien.

Die in § 319 a RVO nicht näher bestimmten Grenzen der Ermächtigung zum Erlaß einer Rechtsverordnung sind aus dem Sinnzusammenhang der Norm mit anderen Vorschriften und aus dem Ziel, das das Krankenversicherungs-Kostendämpfungsgesetz (KVKG) insgesamt verfolgt, zu ermitteln. Diese Grenzen müssen in der zu erlassenden Rechtsverordnung ihren Niederschlag finden. Ich halte es deshalb für erforderlich, daß die Rechtsverordnung nicht nur Inhalt und Form des Mitgliederverzeichnisses bestimmt, sondern auch verbindlich festlegt, für welche konkreten, aus den Zielen des KVKG folgenden Aufgaben — nämlich Dämpfung der Ausgabenentwicklung und Strukturverbesserung in der gesetzlichen Krankenversicherung — die in dem Verzeichnis enthaltenen Aufzeichnungen insgesamt oder in Teilen zu verwenden sind. Erst nach dieser Konkretisierung der Aufgaben läßt sich die Erforderlichkeit und damit die Zulässigkeit der Erfassung der in dem Datenkatalog enthaltenen Einzelangaben beurteilen. Schon jetzt erscheint mir allerdings der Umfang des Datenkatalogs mit über 200 Datenarten außerordentlich weitgehend. Für äußerst problematisch halte ich die Aufzeichnung von Diagnosen in zahlreichen Verwendungszusammenhängen. Zumindest fragwürdig erscheinen mir auch z. B. Angaben über Titel, Geburtsname, Geburtsort, Staatsangehörigkeit, Heilverfahren und Kuren anderer Versicherungsträger, Tätigkeit und Beruf, Ablehnung der Rente und in diesem Zusammenhang Angaben über Art der Entscheidung, Klageerhebung, Klagerücknahme und Urteil.

Bei der Ermittlung des Umfangs der Verordnungsermächtigung und des daraus sich ergebenden Inhalts des Mitgliederverzeichnisses kann m. E. auch die Fortentwicklung des Datenschutzes in anderen Bereichen nicht außer acht gelassen werden. Ich erinnere in diesem Zusammenhang an die langwierigen Verhandlungen zum Melderechtsrahmengesetz; in diesem weit weniger sensiblen Bereich ist u. a. auch der Datenkatalog eingeschränkt worden. Zwar besteht zwischen Melderegister und Mitgliederverzeichnis der Krankenkasse kein unmittelbarer sachlicher und rechtlicher Zusammenhang, doch zeigt dieser Vergleich, daß der Gesetzgeber es für notwendig erachtet, Datensammlungen selbst in relativ „harmlosen" Bereichen auf das unumgänglich erforderliche Maß zu beschränken. Erst recht muß dies dort gelten, wo es um die gesundheitliche und sozialversicherungsrechtliche Situation und nicht zuletzt um das rechte Verhältnis Arzt-Patient-Krankenkasse eines Großteils der Bevölkerung geht. Im übrigen bezweifle ich, ob eine Kostendämpfung im Gesundheitswesen durch Perfektionierung der Kontrolle überhaupt erreicht werden könnte.

Presseberichte, aus denen der BMA den falschen Schluß gezogen hatte, ich hätte meine Bedenken vorzeitig in die Öffentlichkeit getragen, ohne mich vorher um Aufklärung zu bemühen, haben in der Folge leider zu einem unerfreulichen und unnötigen Schriftwechsel vorwiegend über die vermeintlich unkorrekte Form meines Vorgehens geführt, der die notwendige sachliche Diskussion weitgehend in den Hintergrund gedrängt hat. Ohne auf mein Anliegen inhaltlich einzugehen, hat mir der Bundesminister für Arbeit lediglich mitgeteilt, daß die angebliche Absicht, den gesamten Datenkatalog zum Gegenstand einer Rechtsverordnung über das Mitgliederverzeichnis zu machen, unzutreffend sei. Bei diesem Katalog handele es sich um eine Auflistung der bei den Trägern der gesetzlichen Krankenversicherung im wesentlichen anfallenden Daten. Sie sei erstellt worden, um mit den Spitzenverbänden zu erörtern, welche dieser Daten zur rechtmäßigen Erfüllung der Aufgaben der Krankenkassen erforderlich und deshalb in das Mitgliederverzeichnis aufzunehmen seien. Es sei beabsichtigt, mich zu unterrichten, sobald die Vorüberlegungen unter Auswertung der erbetenen Stellungnahmen der Spitzenverbände der Krankenkassen zu Ergebnissen geführt hätten.

Inzwischen ist mir auf Umwegen bekannt geworden, daß diese Stellungnahmen nunmehr vorliegen.

Eine sinnvolle und konstruktive Erfüllung meiner Beratungsaufgabe (§ 19 Abs. 1 BDSG) wird mir nahezu unmöglich gemacht, wenn ich nicht rechtzeitig über Planungen solcher Art unterrichtet werde. Jüngste Gespräche mit der Leitung des Bundesarbeitsministeriums lassen erfreulicherweise eine veränderte Haltung des BMA in Fragen der Zusammenarbeit erkennen. Außerdem habe ich dabei den Eindruck gewonnen, daß der Erlaß einer Rechtsverordnung nach § 319 a RVO gegenwärtig nicht mehr als eine der vordringlichsten Aufgaben angesehen wird.

2.14.6 Eingaben

Zahlreiche Eingaben mit unterschiedlichsten Anliegen und die dadurch ausgelösten Aktivitäten meiner Dienststelle haben in vielen Einzelfällen und Einzelfragen zu einer Verbesserung des Datenschutzes beigetragen. So konnte z. B. erreicht werden, daß Krankenkassen bei der notwendigen Er-

mittlung von Einkommensverhältnissen nicht mehr unbedingt auf der Vorlage des Einkommensteuerbescheids bestehen; dieser enthält neben dem erzielten Einkommen viele weitere Angaben über die persönlichen und wirtschaftlichen Verhältnisse des Betroffenen, die für die jeweilige Aufgabenerfüllung der Krankenkasse nicht erforderlich sind.

In anderen Fällen konnte ich den Betroffenen bei der Durchsetzung ihres Auskunftsrechts hinsichtlich der gespeicherten Daten helfen und darüber hinaus erreichen, daß auch Einsicht in ärztliche Gutachten und Berichte gewährt wird. In einem weiteren Fall wurde aufgrund einer Eingabe und auf mein Einschreiten hin zugesichert, Informationen aus einer nicht erforderlichen schriftlichen Datenübermittlung aus den Akten des Empfängers zu entfernen.

2.14.7 Bundesknappschaft

Im Juli des letzten Jahres habe ich eine umfangreiche Kontrolle bei der Bundesknappschaft in Bochum durchgeführt.

Die Bundesknappschaft bildet unter den Trägern der Sozialversicherung insofern eine Ausnahme, als sie sowohl Träger der Rentenversicherung als auch der Krankenversicherung für die in knappschaftlichen Betrieben beschäftigten Arbeitnehmer ist. Ihre Zuständigkeit erstreckt sich auf das gesamte Bundesgebiet. Die Bundesknappschaft unterhält deshalb zahlreiche Geschäfts- und Verwaltungsstellen. Außerdem betreibt sie mehrere eigene Krankenhäuser. Ich habe die Hauptverwaltung, eine Geschäftsstelle und ein Krankenhaus in Bochum datenschutzrechtlich kontrolliert.

Nach dem dabei gewonnenen Gesamteindruck ist die Verarbeitung personenbezogener Daten gut organisiert und der notwendige Schutz der Sozialdaten ausreichend gewährleistet. Verstöße gegen Datenschutzvorschriften, die zu beanstanden gewesen wären, habe ich nicht festgestellt. Einige Schwachstellen und Ungenauigkeiten konnten mit dem internen Datenschutzbeauftragten rasch und einvernehmlich bereinigt werden.

Aus einer Reihe weiterer Feststellungen sind wegen ihrer grundsätzlichen Bedeutung zu nennen:

— Im Bereich Rentenversicherung/Versorgung für die Mitarbeiter der Bundesknappschaft werden auch für die Beamten fiktive Rentenversicherungskonten geführt, die denen der Rentenversicherten entsprechen. Dafür gibt es keine Rechtsgrundlage und auch keine Notwendigkeit. Das fiktive Rentenkonto kann allenfalls in den wenigen Fällen des Ausscheidens aus dem Beamtenverhältnis für eine Nachversicherung Bedeutung erlangen. Eine derartige Vorratsspeicherung halte ich jedoch für unzulässig. Die Bundesknappschaft hat auch bereits Überlegungen angestellt, auf diese Konten künftig zu verzichten.

— Wie fast alle Verwaltungen zeichnet auch die Bundesknappschaft bei allen dienstlichen und privaten Telefongesprächen die vollständigen Zielnummern auf. Ich habe in zahlreichen Zusammenhängen meine Auffassung dargelegt, daß ich die Aufzeichnung der Zielnummer — zumindest bei Privatgesprächen — für Abrechnungszwecke nicht für erforderlich halte (vgl. auch oben Nr. 2.4.4). Zunächst hielt auch die Geschäftsführung der Bundesknappschaft nach Darlegung meiner Argumente die Zielnummer für entbehrlich, wenn das Aufzeichnungsverfahren für dienstliche und private Gespräche getrennt wird. In einer kurz vor Redaktionsschluß eingegangenen Stellungnahme der Geschäftsführung wird jedoch darauf hingewiesen, daß sich das praktizierte Verfahren bewährt habe. Aus dem Kreis der Mitarbeiter seien bisher keine Beanstandungen bekannt geworden. Die von mir vorgeschlagene Trennung der dienstlichen und privaten Gespräche bei der Aufzeichnung würden zu einem erheblichen Kosten-/Verwaltungsaufwand führen. Daher sei die Geschäftsführung der Ansicht, daß die derzeitige Verfahrensweise unbedenklich beibehalten werden könne.

— Für die automatisierte Rentenbearbeitung wird eine sogenannte Antragsstatistik geführt. Dabei wird für jeden Bildschirm, der mehreren Sachbearbeitern zur Verfügung steht, automatisch die Zahl der vorliegenden und bearbeiteten Anträge sowie die durchschnittliche und die fallbezogene Bearbeitungsdauer aufgezeichnet. Das Ergebnis wird monatlich in einer Liste ausgedruckt, die somit die Arbeitsergebnisse für jede Arbeitsgruppe enthält. Die Arbeitsgruppen bestehen im Durchschnitt aus je 3 bis 5 Mitarbeitern, so daß nicht ausgeschlossen werden kann, daß auch das auf einzelne Mitarbeiter bezogene Leistungsergebnis ermittelt wird. Ich habe meine grundsätzlichen Bedenken gegen eine derartige maschinelle Leistungserfassung und Leistungskontrolle geltend gemacht (vgl. auch 3. TB S. 29).

— Die Knappschaftskrankenhäuser werden als organisatorisch und wirtschaftlich eigenständige Betriebe ohne Rechtspersönlichkeit geführt. Sie sind Teil — d. h. unselbständige Abteilungen — der Bundesknappschaft. Ihre Verwaltungen unterstehen deren Weisungen.

  Die Knappschaftskrankenhäuser erfüllen gleichzeitig die Funktion von allgemeinen Krankenhäusern im Sinne der Landeskrankenhausgesetze. Unter Hinweis auf diese Funktion wird von der Bundesknappschaft die Anwendbarkeit der Vorschriften des Sozialgesetzbuches und des Bundesdatenschutzgesetzes und damit die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz und des Datenschutzbeauftragten der Bundesknappschaft in Frage gestellt (ohne daß deswegen meine Kontrolltätigkeit behindert wurde).

  Als Leistungsträger (§§ 12, 21 SGB I) unterliegt die Bundesknappschaft und damit auch das rechtlich unselbständige Knappschaftskrankenhaus den Vorschriften über die Wahrung des So-

zialgeheimnisses (§ 35 SGB X) und über den Schutz der Sozialdaten (§§ 67 bis 77 SGB X) sowie nach Maßgabe des § 79 SGB X den Vorschriften des 1. und 2. Abschnitts des BDSG. Daraus folgt, daß sowohl der Bundesbeauftragte wie auch der interne Datenschutzbeauftragte die Einhaltung der Datenschutzvorschriften in den Knappschaftskrankenhäusern zu überwachen hat.

Ich werde die Gespräche mit der Bundesknappschaft fortsetzen, um die noch offenen angesprochenen und sonstigen Fragen weiter zu erörtern bzw. abschließend zu klären. (Bis Redaktionsschluß für diesen Bericht lag mir die schriftliche Stellungnahme des Vorstandes der Bundesknappschaft noch nicht vor.)

2.14.8 DVDIS

In meinem Ersten (S. 33), Zweiten (S. 35) und Dritten Tätigkeitsbericht (S. 41) habe ich über das Projekt „Datenerfassung, Verarbeitung, Dokumentation und Informationsverbund in den sozialärztlichen Diensten mit Hilfe der elektronischen Datenverarbeitung" — DVDIS — der Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (AGK) berichtet.

Ursprüngliche Befürchtungen, DVDIS sei Wegbereiter einer medizinischen Bürgerdatenbank — in zentraler oder dezentraler Organisationsstruktur — haben sich als unbegründet erwiesen. Dies vor allem deshalb, weil die AGK diese Befürchtungen schon frühzeitig durch Einschaltung externer Sachverständiger und durch eine intensive Zusammenarbeit mit meiner Dienststelle zerstreuen konnte.

Mit den Fortschritten des Projektes hat sich die Beratung meiner Dienststelle im wesentlichen auf zwei Probleme konzentriert:

- den Aufbau des vorgesehenen Datensatzes,
- ein maschinelles Verfahren bei den Krankenkassen (sogenanntes Auswahlraster), das die Auswahl der Personen vornehmen sollte, die bei den Vertrauensärztlichen Diensten vorzuladen sind.

Die AGK hat mir in einem Schreiben vom Oktober 1982 zugesagt, daß das Auswahlraster nicht eingesetzt wird.

Bezüglich des Datensatzes habe ich Bedenken gegen die Speicherung u. a. folgender Datenfelder angemeldet:

- Rentenversicherungsnummer

  Wie an anderer Stelle dieses Berichts betont, halte ich die administrative Einführung dieser Nummer außerhalb der Rentenversicherung für bedenklich.
- Medikation

  Dieses Feld beantwortet die Frage, welche Medikamente der Patient gegenwärtig einnimmt.
- Familienanamnese
- Psychosoziale Belastung

Auf die Beschreibung von Einzelheiten des komplizierten, für Außenstehende nur mit Mühe verständlichen Konzepts von DVDIS möchte ich hier verzichten. Nach dem jetzigen Stand der Gespräche scheint aber sicher, daß die Felder ‚Medikation', ‚Familienanamnese' und ‚psychosoziale Belastung' nur aus Anlaß der vertrauensärztlichen Begutachtung gespeichert werden sollen. Danach ist ihre Löschung vorgesehen.

Auch nach vieljähriger Projektarbeitszeit besteht noch immer keine ausreichende Klarheit über die Rechtsgrundlagen von DVDIS. Zur Klärung dieser offenbar sehr schwierigen Fragen hat die AGK vor Jahren ein wissenschaftliches Gutachten in Auftrag gegeben, das aber bis jetzt noch nicht vorliegt. So scheint mir zum gegenwärtigen Zeitpunkt eine endgültige Bewertung des Projekts ‚DVDIS' noch nicht möglich.

2.14.9 IDVS II

Das Informations- und Datenverarbeitungssystem für die Ortskrankenkassen (IDVS II) weist noch einige Mängel hinsichtlich der Zugriffskontrolle auf, die mit dem Bundesverband der Ortskrankenkassen (BdO), der das System entwickelt hat, besprochen wurden.

Bei der Kontrolle einer Ortskrankenkasse durch meine Dienststelle war festgestellt worden, daß die Zugriffsbeschränkung nicht ausreichend sicher ist. Gleiches hatte der nordrhein-westfälische Datenschutzbeauftragte festgestellt.

Mein Gespräch mit dem BdO bestätigte diese Feststellungen. Abhilfe wurde zugesagt. Schwerer wiegt jedoch, daß das entwickelte Sicherungssystem offensichtlich von einigen Rechenzentren, die meist bei den Landesverbänden angesiedelt sind, nicht eingesetzt wird. In diesen Fällen kann eine Kasse nicht nur völlig unkontrolliert auf die eigenen Daten zugreifen, sondern auch auf die anderer Kassen.

Eine Stellungnahme des BdO, wie die im System noch vorhandenen Lücken geschlossen werden können und wie der Einsatz des Systems bei allen Rechenzentren sichergestellt werden kann, steht noch aus. Ich kann daher keine abschließende Bewertung vornehmen.

2.15 Unfallversicherung

2.15.1 Allgemeines

Als bundesunmittelbare Träger der Unfallversicherung unterliegen meiner Kontrolle gemäß § 19 Abs. 1 BDSG 32 gewerbliche Berufsgenossenschaften, 5 landwirtschaftliche Berufsgenossenschaften und die See-Berufsgenossenschaft.

Versicherte und Mitglieder bei den Berufsgenossenschaften sind nicht identisch: Versicherte sind

— vereinfacht ausgedrückt — alle unselbständig Beschäftigten und bestimmte selbständig Tätige, Mitglieder dagegen sind die Unternehmer, die auch die Mittel für die Ausgabe der Unfallversicherung (Beiträge) aufzubringen haben.

Als Leistungen der gesetzlichen Unfallversicherung erhalten die Versicherten nach Eintritt eines Arbeitsunfalles insbesondere Heilbehandlung, Verletztengeld oder Übergangsgeld, besondere Unterstützungen, Wiederherstellung oder Erneuerung von Körperersatzstücken, Berufshilfe, Verletztenrente, Sterbegeld und Rente an Hinterbliebene. Darüber hinaus haben Unfallverhütung, Arbeitsschutz und die Erforschung der Berufskrankheiten zunehmend Bedeutung erlangt.

Das Recht der gesetzlichen Unfallversicherung zeichnet sich durch eine relativ große Beständigkeit aus. Die grundlegenden Vorschriften der RVO waren in den letzten Jahren, anders als etwa die Vorschriften über die Krankenversicherung und über die Rentenversicherung, keinen wesentlichen Wandlungen unterworfen.

Auch bei den Berufsgenossenschaften hat sich die automatisierte Datenverarbeitung in weiten Bereichen durchgesetzt. Die eigentliche Unfall- und Leistungsbearbeitung geschieht zwar nach wie vor in konventionellen Akten-Verfahren. Daneben gibt es jedoch zahlreiche Anwendungsgebiete für die automatisierte Datenverarbeitung, so z. B. das Mitglieder- und Beitragswesen, den Zahlungsverkehr, Statistiken, das Personal- und Gehaltswesen, mit zahlreichen Einzeldateien.

Die technische Entwicklung der Datenverarbeitung bei den Berufsgenossenschaften ist nach meinem Eindruck, wohl auch wegen der überwiegend geringeren Größe der Organisationseinheiten, nicht mit der Entwicklung bei den anderen Trägern der Sozialversicherung zu vergleichen: Überwiegend sind noch Rechenzentren anzutreffen, die ausschließlich im Batch-Betrieb arbeiten. Da ich im Vergleich mit anderen Versicherungszweigen nur wenige Kontrollen durchgeführt habe, konnte ich mir keinen Gesamtüberblick verschaffen. Bei den besuchten Berufsgenossenschaften habe ich jedenfalls keine Dialogsysteme angetroffen.

Die vorhandenen „herkömmlichen" Rechenzentren sind sehr unterschiedlich organisiert. Während bei kleineren aus personellen Gründen nicht einmal das Vieraugenprinzip durchzuführen ist, sind andere nach meinem Eindruck organisatorisch gut strukturiert. Dort sind z. B. die Kontrolle der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme (§ 15 Nr. 2 BDSG) u. a. durch Gegenüberstellung von Arbeitsaufträgen und Konsolprotokollen oder die Abgangskontrolle (Nr. 2 der Anl. zu § 6 BDSG) durch eine zuverlässige Datenträgerverwaltung gewährleistet.

Bei den Rechenzentren, in denen ein solcher organisatorischer Stand noch nicht erreicht ist, habe ich mich bemüht, zusammen mit den kontrollierten Stellen unter Berücksichtigung der Verhältnismäßigkeit Lösungen zu finden, die ein höchstmögliches Maß an Sicherheit versprechen, wie z. B. Motivation, Schulung der betroffenen Mitarbeiter, aber auch Kontrollen durch die Geschäftsführung.

Intensive Gespräche habe ich geführt mit der Arbeitsgemeinschaft der Bau-Berufsgenossenschaften hinsichtlich der Entwicklung eines EDV-Systems zur Steuerung des arbeitsmedizinischen Dienstes. Darauf wird im folgenden noch eingegangen.

2.15.2 Zusammenfassender Überblick über die Jahre 1978 bis 1982

Während meiner bisherigen Amtszeit haben meine Mitarbeiter folgende Berufsgenossenschaften kontrolliert:

— See-Berufsgenossenschaft in Hamburg

— Berufsgenossenschaft für den Einzelhandel in Bonn

— Verwaltungs-Berufsgenossenschaft in Hamburg

— Bau-Berufsgenossenschaft in Hamburg.

Bei der Ankündigung einer der ersten Kontrollen wurde meine Kontrollbefugnis bei Körperschaften des öffentlichen Rechts in Zweifel gezogen. Dieses Mißverständnis konnte jedoch im Benehmen mit dem Hauptverband der gewerblichen Berufsgenossenschaften rasch ausgeräumt werden. Dann war auch in diesem, wie in allen anderen Fällen, die Zusammenarbeit mit den kontrollierten Stellen gut. Die Bereitschaft, meine Vorstellung und Vorschläge aufzunehmen und nach den jeweils gegebenen Möglichkeiten in die Praxis umzusetzen, war bei allen Stellen vorhanden.

Der Stand der Durchführung des Datenschutzes und der Datensicherung war recht unterschiedlich, so daß ich darüber keine generalisierbaren Aussagen machen kann. Bei einer Berufsgenossenschaft habe ich eine sehr gute Organisation des Datenschutzes mit einer sachgerechten Verteilung der Verantwortlichkeiten zwischen EDV- und Fachabteilungen angetroffen. Bei anderen Berufsgenossenschaften waren die vorgefundenen Datenschutz- und Datensicherungskonzepte weitgehend unzureichend und mußten neu durchdacht und neu entwickelt werden.

Häufiger festgestellte Mängel waren:

— Formulare, mit denen Daten beim Betroffenen erhoben werden, enthielten den in § 9 Abs. 2 BDSG vorgeschriebenen Hinweis auf die Rechtsgrundlage der Erhebung bzw. auf die Freiwilligkeit der Angaben nicht oder nicht in ausreichender bzw. für den Betroffenen verständlicher Form.

— Die nach § 15 Abs. 1 BDSG erforderliche Übersicht über die Art der gespeicherten Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger war unvollständig oder falsch angelegt oder überhaupt nicht vorhanden.

— Wesentliche, in der Anlage zu § 6 Abs. 1 Satz 1 BDSG genannte technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes waren nicht getroffen oder unzureichend.

— Der Objektschutz des Rechenzentrums war unzureichend.

Im einzelnen habe ich darüber in den bisherigen vier Tätigkeitsberichten berichtet (1. TB S. 35, 2. TB S. 35, 3. TB S. 41, 4. TB S. 16, 17).

2.15.3 Verwendung der Rentenversicherungsnummer im Arbeitsmedizinischen Dienst der Bau-Berufsgenossenschaften

Die Bau-Berufsgenossenschaften beabsichtigen, die Rentenversicherungsnummer als Ordnungs- und Identifizierungsmerkmal beim Aufbau eines künftigen automatisierten Systems für die arbeitsmedizinische Betreuung der Bauarbeiter zu benutzen. Über meine Bedenken gegen dieses Vorhaben habe ich schon im 3. Tätigkeitsbericht (3. TB S. 41 f.) berichtet.

In den jahrelangen Erörterungen mit den Bau-Berufsgenossenschaften ging es im wesentlichen um zwei Probleme:

— Ich sehe in der Verwendung dieser Nummer außerhalb der Rentenversicherung ein Risiko für die Privatsphäre des einzelnen Bürgers und für die Gesellschaft insgesamt. Die Berufsgenossenschaften konnten sich meinen Argumenten nicht verschließen.

— Fraglich war, ob es organisatorisch und finanziell befriedigende Alternativen gibt, falls die Bau-Berufsgenossenschaften auf die Verwendung der Rentenversicherungsnummer verzichten und ein anderes Identifizierungsmerkmal benutzen.

Nach langwierigen Verhandlungen, an denen zeitweise auch die Parlamentarischen Staatssekretäre des Bundesarbeitsministeriums (der früheren Bundesregierung) beteiligt waren, erscheinen mir die grundlegenden Probleme entscheidungsreif.

Der Rechtsausschuß des Deutschen Bundestages hat in seiner Sitzung vom 5. Mai 1976 aus verfassungs- und rechtspolitischen Gründen die Entwicklung, Einführung und Verwendung von Numerierungssystemen, die eine einheitliche Numerierung der Gesamtbevölkerung ermöglichen (Personenkennzeichen), für unzulässig erklärt (vgl. auch Nr. 2.1.1 dieses Berichts). Daraufhin sind Pläne, ein Personenkennzeichen im Rahmen eines Bundesmeldegesetzes einzuführen, nicht weiterverfolgt worden.

Am 26. Oktober 1977 wurde aus der Mitte des Bundestages der Entwurf eines Gesetzes zur Änderung der Reichsversicherungsordnung eingebracht (Drucksache 8/1086). Dieser Entwurf ist zwar nicht weiterverfolgt worden, doch sind seine tragenden Gedanken und die Lösungsvorschläge im Prinzip auch heute noch aktuell:

Nach § 319 Abs. 2 RVO ist der Bundesminister für Arbeit und Sozialordnung ermächtigt, den Aufbau und den Zeitpunkt der Einführung der Rentenversicherungsnummer durch Rechtsverordnung festzulegen. Der erwähnte Gesetzentwurf sollte die Bildung einer einheitlichen Versicherungsnummer für alle Versicherten im Bundesgebiet verhindern und sicherstellen, daß die krankenkassen-eigene Nummer nur aufgabenbezogen verwendet und weitergegeben werden darf. Der Entwurf stützte sich inhaltlich auf das Argument, daß die Rentenversicherungsnummer „technisch einem allgemeinen Personenkennzeichen nahe"-komme und ein darauf aufbauendes Datensystem „nicht dem verfassungsrechtlich garantierten Schutz der Persönlichkeit" entspreche und „insbesondere psychologisch nicht mehr abwägbare Auswirkungen auf das Verhalten der Versicherten" habe. Es kann kein vernünftiger Zweifel bestehen, daß diese Risiken für die Privatsphäre der Bürger auch heute noch bestehen. Hinzu kommt ein weiteres, eher strukturelles Risiko: Die gesetzliche Sozialverwaltung erfaßt heute etwa 90 % der Gesamtbevölkerung. Eine gemeinsame Nummer für diesen großen, schon jetzt kaum mehr überschaubaren Bereich hätte zur Konsequenz, daß die Vielfalt der unterschiedlichen Informationsprozesse und unterschiedlichen Interessen nach einem einheitlichen Prinzip organisiert wäre. Es ist darüber hinaus davon auszugehen, daß Dritte, zu denken wäre etwa an Arbeitgeber oder Ärzte, ihre Bestände mit dem gleichen Ordnungsmerkmal organisieren. Das Risiko einer derartigen Entwicklung sehe ich — in Übereinstimmung mit vergleichbaren ausländischen Erfahrungen — in der Unüberschaubarkeit des so entstehenden Systems von Informationsbeziehungen und den fehlenden Möglichkeiten, die einmal entstandene Organisationsstruktur je nach politischem Willen jemals noch zu ändern. Schon aus Kostengründen wäre dies nicht durchsetzbar. Die möglichen Gefährdungen für die Freiheit des einzelnen Bürgers, aber auch für die Freiheitsspielräume insgesamt, die unsere Gesellschaft den Bürgern bietet, halte ich für so groß, daß nach dem Prinzip des Vorbehalts des Gesetzes allein der Gesetzgeber über eine Ausdehnung des Anwendungsbereichs der Rentenversicherungsnummer entscheiden darf — eine verfassungsrechtliche Linie, die das Bundesverfassungsgericht in seinem Kalkar-Beschluß (BVerfGE 49, 89 ff. [127]) vorgezeichnet hat.

Für den Bereich der Berufsgenossenschaften kommt hier noch hinzu, daß § 319 RVO die Berufsgenossenschaften als mögliche Adressaten überhaupt nicht erwähnt.

In meiner ablehnenden Haltung bestärkt mich die Einsicht, daß es, jedenfalls im Bereich der Bau-Berufsgenossenschaften, Alternativen gibt, die die ordnungsgemäße Aufgabenerfüllung nicht beeinträchtigen: Ordnungssysteme wie die Rentenversicherungsnummer haben den Zweck, Doppel- und Mehrfachvergaben auszuschließen sowie eindeutige Verbindungen zwischen Personen und den über sie gespeicherten Daten herzustellen. Dabei ist es ohne weiteres möglich, *für verschiedene Aufga-*

benbereiche auch verschiedene Ordnungsysteme zu verwenden, die dann auch an den speziellen Erfordernissen ausgerichtet sein können. Ein entsprechendes Modell habe ich den Bau-Berufsgenossenschaften vorgeschlagen.

Bei den Gesprächen mit den Vertretern der Bau-Berufsgenossenschaften bestand Einvernehmen, daß dieses Gedankenmodell realisierbar und vielleicht sogar betroffenenfreundlicher ist und heilsame dezentralisierende Wirkungen entfalten kann. Für den etwaigen praktischen Einsatz sind jedoch weitere Untersuchungen erforderlich. Ich habe Verständnis dafür, daß die Berufsgenossenschaften zunächst abwarten wollen, ob sich der Gesetzgeber für oder gegen die Verwendung der Rentenversicherungsnummer außerhalb der Rentenversicherung entscheidet.

Ich appelliere daher an den Deutschen Bundestag, in Abwägung aller Vorteile und Risiken über das Ob und Wie zu befinden. Diese Entscheidung ist eilbedürftig, wenn verhindert werden soll, daß die Rentenversicherungsnummer in zunehmend mehr, wenn auch für sich unbedeutenden Zusammenhängen administrativ eingeführt wird.

2.15.4 Arbeitsstoffverordnung

Die Arbeitsstoffverordnung vom 29. Juli 1980 (BGBl. I S. 1071), die sich mit dem Umgang mit gefährlichen Arbeitsstoffen und mit der gesundheitlichen Überwachung der dabei beschäftigten Arbeitnehmer befaßt, schreibt in § 19 vor:

> „(1) Für die Arbeitnehmer, die nach dieser Verordnung ärztlich untersucht worden sind, ist von ihrem Arbeitgeber eine Gesundheitskartei zu führen.
>
> (3) Der Arbeitgeber hat die Karteikarte und die ärztlichen Bescheinigungen für jeden Arbeitnehmer bis zu dessen Entlassung aufzubewahren. Danach sind die Karteikarte und die ärztlichen Bescheinigungen dem entlassenen Arbeitnehmer auszuhändigen."

Von dem Datenschutzbeauftragten eines Landes bin ich darauf hingewiesen worden, daß Berufsgenossenschaften den gewerblichen Unternehmern empfehlen, auch nach dem Ausscheiden eines Arbeitnehmers die Gesundheitskarte aufzubewahren; Unfallverhütungsvorschriften sähen im Gegensatz zu der Arbeitstoffverordnung vor, daß beim Ausscheiden eines Arbeitnehmers die Gesundheitskarte vom Arbeitgeber der Berufsgenossenschaft zu übergeben sei.

Dazu habe ich den Bundesminister für Arbeit und Sozialordnung und den Hauptverband der gewerblichen Berufsgenossenschaften um Stellungnahme gebeten. Die Stellungnahmen zu meiner ersten Anfrage und zu notwendig gewordenen Rückfragen sind sehr zögerlich und zum Teil erst nach weiterer Erinnerung eingegangen. Zehn Monate nach meiner ersten Anfrage ist es mir noch nicht gelungen, eine einvernehmliche Klärung der Sach- und Rechtslage herbeizuführen. Die bisherigen Stellungnahmen sind widersprüchlich und im Ergebnis nicht befriedigend:

Die Zentralstelle für Unfallverhütung und Arbeitsmedizin beim Hauptverband der gewerblichen Berufsgenossenschaften hat mir zunächst mitgeteilt, die Unfallverhütungsvorschrift „Schutz gegen gesundheitsgefährlichen Staub" (VBG 119) sehe in § 17 vor, daß die Gesundheitskarte (nach dem Ausscheiden des Arbeitnehmers) der Berufsgenossenschaft zu übergeben sei. Da die VBG 119 nach ihrem § 1 Abs. 2 aber nicht gelte, soweit ihr Gegenstand durch staatliche Rechtsvorschrift geregelt sei, träten die einschlägigen Regelungen in § 17 der VBG 119 gegenüber § 19 der Arbeitsstoffverordnung zurück.

Aus dieser Stellungnahme habe ich den Schluß gezogen, daß auch nach Auffassung der Zentralstelle und des BMA, der sich dieser Stellungnahme angeschlossen hatte, nach dem Inkrafttreten der Arbeitsstoffverordnung am 1. Oktober 1980 § 17 der VBG 119 nicht mehr angewendet würde und folglich ab diesem Zeitpunkt die Gesundheitskarte und die ärztlichen Bescheinigungen dem Arbeitnehmer nach seinem Ausscheiden ausgehändigt werden.

Im weiteren Verlauf des Schriftwechsels hat mir der BMA jedoch mitgeteilt, daß von einem Vorrang der Rechtsverordnung keine Rede sei. Rechtsverordnung und Unfallverhütungsvorschrift würden sich hinsichtlich der Regelung der gesundheitlichen Überwachung nicht überschneiden, da nur die Unfallverhütungsvorschrift eine Regelung über die gesundheitliche Überwachung beim Umgang mit gesundheitsgefährlichem mineralischen Staub enthalte. Dieser Stellungnahme hat sich die Zentralstelle nunmehr „voll inhaltlich" angeschlossen.

Nach meiner Auffassung regeln beide Vorschriften den gleichen Gegenstand mit der Folge, daß deshalb die Regelung der VBG 119 über die Übergabe der Gesundheitskarte an die Berufsgenossenschaft wegen des Vorranges der Arbeitsstoffverordnung nicht gilt (§ 1 Abs. 2 VBG 119).

Die Führung der Gesundheitskartei (Speicherung personenbezogener Daten) und ihre Übergabe an die Berufsgenossenschaft (Übermittlung) ist nach § 3 Satz 1 BDSG nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.

Die Speicherung ist zulässig, weil § 19 Arbeitsstoffverordnung sie vorschreibt (zuläßt). Die Zulässigkeit der Speicherung endet jedoch mit dem Ausscheiden des Arbeitnehmers, weil § 19 Abs. 3 der Arbeitsstoffverordnung für diesen Fall die Aushändigung des Datenträgers (Karteikarte) an den Arbeitnehmer und damit die „Löschung" bei der speichernden Stelle vorschreibt.

Aufgrund dieser Rechtslage halte ich die Aufbewahrung der Gesundheitskarte beim Arbeitgeber auch nach dem Ausscheiden des Arbeitnehmers sowie die Übergabe an die Berufsgenossenschaft für unzulässig und sehe darin einen Verstoß gegen datenschutzrechtliche Vorschriften.

2.15.5 Offenbarung medizinischer Daten

Mehrfach wurde in Einzeleingaben an mich die Frage herangetragen, ob es zulässig sei, daß die Berufsgenossenschaft einem von ihr beauftragten ärztlichen Gutachter ihre Akten über den betroffenen Versicherten zur Verfügung stellt, einschließlich der darin enthaltenen anderen ärztlichen Gutachten, Berichte und Befunde.

Dazu ist zunächst festzustellen, daß alle Einzelangaben über die persönlichen und sachlichen Verhältnisse eines Versicherten bei der Berufsgenossenschaft als Sozialgeheimnis zu wahren sind und nicht unbefugt einem Dritten offenbart werden dürfen. Die Zulässigkeit der Offenbarung richtet sich ausschließlich nach den in den §§ 67 bis 77 SGB X festgelegten Voraussetzungen. In Betracht kommt hier — neben der Einwilligung des Betroffenen im Einzelfall — die Vorschrift des § 69 Abs. 1 Nr. 1 SGB X. Danach ist die Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch die Berufsgenossenschaft erforderlich ist.

Unzweifelhaft gehört zu diesen Aufgaben der Berufsgenossenschaft die Feststellung von Unfallfolgen und die dafür notwendige Begutachtung durch einen ärztlichen Sachverständigen. Eine Einschränkung der insoweit gegebenen Offenbarungsbefugnis ergibt sich jedoch bereits daraus, daß die Offenbarung nur zulässig ist, soweit sie für die Erfüllung dieser Aufgabe erforderlich ist. Eine weitere Einschränkung ergibt sich gegebenenfalls aus der ärztlichen Schweigepflicht. Wenn sich in der Akte ärztliche Gutachten, Berichte, Befunde und andere medizinische Angaben befinden, die der Berufsgenossenschaft von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person zugänglich gemacht worden sind, dann dürfen diese Angaben dem beauftragten Gutachter nur unter den Voraussetzungen mitgeteilt (offenbart) werden, unter denen diese Person selbst offenbarungsbefugt wäre (§ 76 Abs. 1 SGB X). Nach den zu der ärztlichen Schweigepflicht entwickelten Grundsätzen ist dafür die Einwilligung des Patienten erforderlich, soweit nicht eine gesetzliche Mitteilungspflicht besteht oder die Offenbarung unter den Voraussetzungen des § 34 StGB (rechtfertigender Notstand) zum Schutze eines höheren Rechtsgutes erforderlich ist.

Diese besondere Einschränkung der Offenbarungsbefugnis, bezogen auf die ärztliche Schweigepflicht desjenigen, von dem die ärztlichen Unterlagen in den Unfallakten stammen (die Berufsgenossenschaft selbst unterliegt in der Regel der ärztlichen Schweigepflicht nicht), gilt nach § 76 Abs. 2 SGB X im Rahmen der Aufgabenerfüllung durch die Berufsgenossenschaft nicht für Angaben, die der Berufsgenossenschaft im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistungen (dazu gehören auch die Geldleistungen für die Folgen eines Arbeitsunfalles) oder wegen der Ausstellung einer Bescheinigung mitgeteilt worden sind. Allerdings kann der Betroffene in diesen Fällen der Offenbarung widersprechen.

Der mögliche Widerspruch setzt aber die Kenntnis des Betroffenen von der beabsichtigten Offenbarung voraus. Der Betroffene muß also über die beabsichtigte Aktenversendung aufgeklärt werden. Widerspricht er, verstößt er damit unter Umständen gegen seine Mitwirkungspflichten bei der Beantragung von Sozialleistungen (§§ 60 bis 65 SGB X). Auch hierüber und über die Folgen fehlender Mitwirkung (§ 66 SGB X), nämlich die mögliche Ablehnung der beantragten Leistungen, ist er aufzuklären.

Dies alles zeigt, daß die unbesehene routinemäßige Übersendung der Unfallakte an einen ärztlichen Gutachter nicht zulässig sein kann. Die Berufsgenossenschaft muß in jedem Einzelfall prüfen, ob und gegebenenfalls in welchem Umfang die Kenntnis der Aktenunterlagen für den Gutachter erforderlich ist und ob für die Übersendung bestimmter Aktenteile die Einwilligung des Betroffenen einzuholen ist.

2.15.6 Bewertung und Ausblick

Nach meinen, in diesem Bereich allerdings mehr punktuellen Erfahrungen, bietet die Datenverarbeitung bei den Trägern der gesetzlichen Unfallversicherung keinen besonderen Anlaß zu genereller Sorge. Die Datenübermittlungen (Offenbarungen) an andere Stellen innerhalb und außerhalb der Sozialverwaltung sind im allgemeinen auf das erforderliche Ausmaß beschränkt. Zu erkennbaren Mißbräuchen und Beeinträchtigungen schutzwürdiger Belange der Betroffenen ist es nach meinen Feststellungen nicht gekommen.

Die mehrfach festgestellten Mängel in organisatorischer und technischer Hinsicht schließen allerdings die Möglichkeit einer mißbräuchlichen Verwendung der gespeicherten Daten nicht aus. Ich habe deshalb bei meinen Kontrollen stets besonderen Wert darauf gelegt, im Benehmen mit den kontrollierten Stellen nach Lösungen zu suchen, die solche Mängel ohne unvertretbar hohen Aufwand beseitigen. Meine Anregungen wurden in aller Regel bereitwillig aufgenommen.

Nicht ganz so positiv kann ich die Durchsetzung des Datenschutzes in der täglichen Verwaltungsroutine beurteilen. Die Bereitschaft bzw. die Kenntnis der rechtlichen Verpflichtung, dem Betroffenen gegenüber die Erforderlichkeit und den Umfang der Erhebung und Verarbeitung seiner oft intimen Daten offenzulegen, läßt in vielen Fällen zu wünschen übrig. Dies zeigt sich z. B. darin, daß Datenübermittlungen in Einzelfällen ohne die notwendige Einwilligung des Betroffenen oder sogar gegen dessen ausdrücklich erklärten Willen stattfinden, oder insbesondere in der häufig noch mangelhaften datenschutzgerechten Gestaltung von Vordrucken, mit denen Daten beim Betroffenen erhoben werden.

Der in § 9 Abs. 2 BDSG vorgeschriebene Hinweis auf die Rechtsvorschrift, die den Betroffenen verpflichtet, die gewünschten Angaben zu machen, bzw. auf die Freiwilligkeit seiner Angaben fehlt oft ganz oder ist so knapp oder auch fehlerhaft formu-

liert, daß der Betroffene damit nichts anfangen kann.

Ich halte es für ein besonders wichtiges Anliegen des Datenschutzes, die Datenverarbeitung für den Betroffenen transparent zu machen. Es ist deshalb eine bleibende Aufgabe für jede einzelne Berufsgenossenschaft und insbesondere für deren internen Datenschutzbeauftragten, diese Transparenz herzustellen oder noch wirksamer zu machen. Dies kann z. B. durch entsprechende Schulung der Mitarbeiter und eine dem Sinn des § 9 Abs. 2 BDSG entsprechende Gestaltung der notwendigen Hinweise auf den Erhebungsvordrucken gewährleistet werden.

2.16 Gesundheitswesen

Meine Zuständigkeiten für den Datenschutz im Gesundheitswesen sind — entsprechend den eingeschränkten Zuständigkeiten des Bundes — begrenzt. Die wesentlichen Konflikte der letzten Jahre sind in einzelnen Bundesländern aufgetreten und waren dort auszutragen. Meine Aktivitäten in diesem Bereich haben sich deshalb darauf konzentriert, das Anliegen des Datenschutzes in den bundesweiten Verbänden der Ärzte, Kassen und Standesvertretungen einzubringen. Im übrigen haben die Datenschutzbeauftragten des Bundes und der Länder einen Arbeitskreis „Sozialwesen" geschaffen, der dem Meinungsaustausch und der Entscheidungsvorbereitung u. a. über Probleme des Gesundheitswesens dient.

Besonders hervorzuheben sind jedoch die Überprüfung des Bundesgesundheitsamtes in Berlin und die Mitarbeit an dem Musterentwurf für ein Krebsregistergesetz.

2.16.1 Bundesgesundheitsamt

Im Jahre 1980 hatte ich beim Bundesgesundheitsamt schwerwiegende Mängel bei der Umsetzung des Datenschutzes festgestellt. Diese Mängel haben damals zum Abbruch einer Kontrolle geführt.

Im Frühjahr 1981 habe ich das Bundesgesundheitsamt nochmals überprüfen lassen, um mir ein Bild von den erzielten Fortschritten zu machen. Gegenstand dieser Kontrolle waren ausschließlich technisch-organisatorische Fragen des Datenschutzes, um die Risiken der Datenverarbeitung beim Bundesgesundheitsamt für die Bürger besser einschätzen zu können. Ich konnte mich bei diesem Besuch davon überzeugen, daß das Bundesgesundheitsamt meine früheren Anregungen aufgegriffen und im Rahmen seiner Möglichkeiten beseitigt hat.

Das Rechenzentrum des Bundesgesundheitsamtes war damals in einer Baracke untergebracht und deshalb kaum ausreichend zu sichern. Die damalige Bundesministerin für Jugend, Familie und Gesundheit hat sich persönlich dieser Sache angenommen und die zuständigen Gremien des Deutschen Bundestages um weitere Haushaltsmittel für eine Unterbringung des Rechenzentrums entsprechend modernen Standards gebeten. Bis zur Fertigstellung eines neuen Rechenzentrums wurde eine akzeptable Übergangslösung gefunden.

Wegen des eingegrenzten Prüfungszieles konnten auch bei diesem Besuch einige Probleme nur angesprochen, aber nicht gelöst werden.

Das Bundesgesundheitsamt hat inzwischen eine Risiko- und Schwachstellenanalyse angefertigt, die mir seit September 1982 vorliegt. Sie gibt Aufschluß darüber, wo technische, organisatorische oder rechtliche Maßnahmen erforderlich sind. Sie bietet einen guten Gesamtüberblick, ist differenziert und klar auch in Details und dürfte insoweit beispielhaft auch für andere Anwender sein. Es wird sich zeigen müssen, inwieweit sie in die Praxis umgesetzt wird.

Ich habe dem Bundesgesundheitsamt eine weitere Prüfung für das Jahr 1983 angekündigt.

2.16.2 Entwurf eines Mustergesetzes zur Krebsregistrierung

Der Bundesminister für Jugend, Familie und Gesundheit hat am 8. Februar 1982 das „Muster eines Gesetzes über ein Krebsregister" an die Gesundheitsminister und -senatoren versandt. An diesem Entwurf habe ich in einer dafür eingerichteten Arbeitsgruppe mitgearbeitet. Mit meinen Vorstellungen habe ich mich allerdings in einigen wesentlichen Punkten nicht durchsetzen können. Hierzu verweise ich auf den Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der in meinem Vierten Tätigkeitsbericht auf S. 48 f. abgedruckt ist.

Der Mustergesetzentwurf ist in den vergangenen Monaten in einzelnen Bundesländern und in der beteiligten Fachöffentlichkeit ausführlich diskutiert worden. In Hessen ist ein Gesetzentwurf, der dem Musterentwurf des Bundes in den wesentlichen Punkten folgt, zurückgezogen worden.

Im „Gesamtprogramm zur Krebsbekämpfung" (Fachbereichskommission „Prävention", Arbeitsgruppe „Epidemiologie") sind daraufhin im Anschluß an die „2. Große Krebskonferenz" vom 16. November 1982 „Grundsätze der Krebsregistrierung" entwickelt worden. In Kenntnis dieser Grundsätze hat die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder am 10. Dezember 1982 in Berlin einen Beschluß gefaßt, der nach dem Entwurf wie folgt lautet:

> „Krebsregister
>
> Die für das Gesundheitswesen zuständigen Minister und Senatoren der Länder haben sich mit der Notwendigkeit epidemiologischer Krebsforschung in der Bundesrepublik Deutschland befaßt. Sie haben die Ergebnisse der 2. Großen Krebskonferenz „Grundsätze der Krebsregistrierung" zur Kenntnis genommen.
>
> Sie bitten die Bundesregierung, gemeinsam mit den Ländern den Mustergesetzentwurf zu überarbeiten, damit den Ländern einheitliche Kriterien der Datenerfassung zur Verfügung stehen."

Aufgrund dieser Sachlage gehe ich davon aus, daß im Jahre 1983 ausreichend Gelegenheit sein wird, die Belange von Datenschutz und medizinischer Forschung — besser als im Musterentwurf vom Februar 1982 — aufeinander abzustimmen. Ohne hier abschließend zu den „Grundsätzen der Krebsregistrierung" Stellung nehmen zu wollen, scheinen mir folgende Hinweise angebracht:

1. Es besteht Einvernehmen, daß die Führung regionaler Krebsregister ohne bestimmte rechtliche Grundlagen nicht zulässig ist. Ich begrüße es, daß die „Grundsätze" gegenüber dem Musterentwurf eine erfreuliche Klarstellung in der Zielsetzung dieser Register enthalten.

2. In den „Grundsätzen der Krebsregistrierung" wird festgestellt: „Ein einziges zentrales Register für die Bundesrepublik Deutschland ist nicht anzustreben." Weiter heißt es: „Auf lange Sicht ist eine Flächendeckung der Bundesrepublik Deutschland durch regionale Register anzustreben." Wenn für die regionalen Register eine Organisationsform gewählt wird, die die Zusammenführung der Register erlaubt, halte ich dies für bedenklich. Auch stünde es im Widerspruch zu der erstgenannten Aussage in den Grundsätzen.

3. Es ist sicherzustellen, daß die Krebsregister nur für Zwecke der Krebsforschung personenbezogene Daten sammeln und weitergeben dürfen.

4. In den Grundsätzen heißt es unter Punkt 9: „Für die namentliche Meldung soll die Einwilligung des Patienten nicht generell gefordert werden."

   Diese Position, gegen die ich mich auch in der Vergangenheit immer gewandt habe, überzeugt mich nach wie vor nicht. Mir sind bis jetzt keine überzeugenden Beweise dafür bekannt, daß Krebsregister, die für Meldungen eine Einwilligung der Patienten verlangen, schlechtere Aussagen liefern als die jetzt vorgesehenen Register.

5. Die „Grundsätze" stellen die Forderung auf, personenbezogene Daten möglichst frühzeitig zu anonymisieren. Gedacht ist z. B. an Meldungen an Treuhandstellen bei den Ärztekammern, die personenbezogene Daten mit Hilfe mathematischer Verfahren zu verschlüsseln hätten.

   Diese Überlegungen halte ich für begrüßenswert. Allerdings wird es darauf ankommen, wie derartige Treuhandstellen organisatorisch und rechtlich eingebettet sind.

6. Die „Grundsätze" sehen einen regelmäßigen Datenabgleich zwischen Krebsregistern und Meldebehörden vor. Ein derartiger Datenabgleich bedarf nach meiner Auffassung einer eindeutigen Rechtsgrundlage, die auch Einzelheiten des Verfahrens festlegt.

Insgesamt erkenne ich in den „Grundsätzen der Krebsregistrierung" — trotz der erwähnten Bedenken — einen weiterführenden Schritt zu Lösung der Probleme. Wie schon in der Vergangenheit ist meine Dienststelle bereit, an der Klärung dieser Probleme mitzuarbeiten.

2.17 Wirtschaftsverwaltung und öffentlich-rechtliche Unternehmen

2.17.1 Wirtschaftsverwaltung

Die Datenschutzkontrollen bei den Bundesministerien für Wirtschaft, für Ernährung, Landwirtschaft und Forsten sowie für wirtschaftliche Zusammenarbeit haben gezeigt, daß in diesen Ressorts wegen ihrer vor allem gesetzgeberischen, planenden und aufsichtsführenden Tätigkeit Datensammlungen mit personenbezogenen Angaben — abgesehen von solchen der internen Verwaltung — nur am Rande eine Rolle spielen. Soweit automatisierte Datenverarbeitungssysteme eingesetzt werden, unterstützen sie in erster Linie die eigene Verwaltung und die Arbeit mit Adreßbeständen. Mängel des Datenschutzes, die sich zu Lasten von Betroffenen ausgewirkt haben, wurden bei den Kontrollbesuchen nicht festgestellt. Zur Sicherstellung des Datenschutzes waren im großen und ganzen zufriedenstellende Vorkehrungen getroffen. Gleichwohl habe ich einzelne Schwachstellen ermittelt, die zwar bisher zu keinen Beschwerden Betroffener geführt haben, die aber eine Beeinträchtigung schutzwürdiger Belange möglich erscheinen lassen. Im Einvernehmen mit den jeweiligen Häusern wurden praktikable Lösungen gefunden. Dazu gehören beispielsweise Grundsätze für die Verwendung von Anschriftendateien (vgl. 1 TB S. 39); organisatorische Regelungen für das Führen, Verwalten und Löschen von Dateien, um die Verbreitung von Informationen auf das erforderliche Maß zu beschränken; das Anschaffen bzw. Einrichten zusätzlicher EDV-Sicherungen beim Ausbau der Direkt-Zugriffs-Verarbeitung.

2.17.2 Einrichtung eines Filmförderungsregisters

Die in Bund und Ländern bestehenden Filmförderungseinrichtungen haben entschieden, zur effektiven und zielgerichteten Koordinierung der Förderungsmaßnahmen ein zentrales Register einzurichten. Jede Förderung wird mit 36 Merkmalsbeschreibungen erfaßt und von der jeweiligen Fördereinrichtung dem zentral geführten Register gemeldet. Das Register steht allen Förderern mit Auskünften zur Verfügung.

Bei der datenschutzrechtlichen Beurteilung, ob ein Informationsaustausch durch eine solche zentrale Datensammlung für eine sachgerechte und ordnungsgemäße Filmförderung erforderlich ist oder ob im Hinblick auf die schutzwürdigen Belange der Betroffenen besser auf eine Zentraldatei verzichtet werden sollte, stehen sich die Standpunkte diametral gegenüber. Die Filmförderer verweisen auf Haushaltsvorschriften; die Grundsätze sparsamer Wirtschaftsführung verlangten, dem Subventionsbetrug entgegenzuwirken. Von Seiten der Betroffenen wird geltend gemacht, daß die Förderungspraxis seit zehn Jahren ohne einen gegenseitigen Datenaustausch ausgekommen ist.

Aus der Sicht des Datenschutzes stellt sich u. a. die Frage, inwieweit eine Registrierung aller Anträge — also auch der später im Bewilligungsverfahren

abgelehnten — zu ungerechtfertigten Benachteiligungen von Betroffenen führt. Es muß vermieden werden, daß durch die Auskunft aus dem Register Anträge bei einer anderen Fördereinrichtung nur deshalb abgelehnt werden, weil frühere Anträge des Betroffenen abgelehnt wurden. Die sachliche Prüfung jedes Einzelfalles muß gewährleistet bleiben.

Die Möglichkeit, das Zentral-Register nach verschiedenen Kriterien auszuwerten, darf nicht dazu führen, daß die auskunftsberechtigten Fördereinrichtungen Informationen abrufen, die ihnen aufgrund eigener Aufgabenstellung nicht zuständen.

Zentral geführte Datenbestände sind unter Datenschutzgesichtspunkten besonders sorgfältig daraufhin zu überprüfen, daß erstens nur die für die Zielsetzung des Registers unbedingt notwendigen Einzelangaben zusammengefaßt werden und daß zweitens eine unbefugte Registerbenutzung vermieden wird. Das bedeutet im ersten Fall die Überprüfung, ob alle 36 Positionen sachlich erforderlich sind, und im zweiten Fall eine abschließende Festlegung der Zwecke sowie der Nutznießer des Registers. Der Hinweis darauf erscheint mir notwendig, weil die Generalklauseln der §§ 10, 11 BDSG eine zweckfremde Verwendung der Daten nicht ausschließen. Ein solches Risiko ist nicht unrealistisch, weil zentrale Datenbestände erfahrungsgemäß zusätzliche Informationswünsche erzeugen.

Ein weiterer Datenschutzgesichtspunkt besteht in der Aufklärung des Betroffenen über Einrichtung und Benutzung des Registers. Dem Antragsteller sollte klar sein, welche Angaben zentral gespeichert werden und welche Institutionen Auskünfte erhalten können. Die präventive Wirkung einer solchen Transparenz dürfte auch im Interesse der Filmförderer liegen.

Eine Gruppe betroffener Filmproduzenten hat Bedenken gegen die zentrale Registrierung angemeldet. Der Vorgang ist noch nicht abgeschlossen.

2.17.3 Deutsche Bundesbank

Die Deutsche Bundesbank war seit Verabschiedung des BDSG bemüht, die nach § 16 BDSG erforderlichen geschäftsbezogenen Regelungen zur Gewährleistung des Datenschutzes zu entwickeln und sie in eine umfassende Datenschutz-Konzeption zu bringen.

Bei meinem Kontrollbesuch im Jahre 1981 hatte ich den Eindruck gewonnen, daß die Bundesbank auf dem Gebiet der Organisation des Datenschutzes Hervorragendes geleistet hat (vgl. 4. TB S. 19). Auf das vorbildliche Regel- und Dokumentations-System habe ich auch andere Stellen aufmerksam gemacht und empfohlen, die Erfahrungen der Bundesbank zu nutzen.

Die Deutsche Bundesbank ist auch ein Beispiel dafür, daß die Sicherstellung des Datenschutzes als permanente Aufgabe mit geringem Aufwand erreichbar ist.

Die kritischen Feststellungen zu einzelnen Vorgängen anläßlich meiner Prüfung sind — bis auf einen Fall — gegenstandslos geworden: Dem Gebot der Aufklärung (§ 9 Abs. 2 BDSG und § 11 Abs. 3 BStatG) im Zusammenhang mit der Erhebung und weiteren Verwendung von Daten nach dem Außenwirtschaftsgesetz wird durch Änderungen der Vordrucke Rechnung getragen; die Bedenken gegen die Rechtmäßigkeit der Erhebung der Laufzeiten von Millionen-Krediten (Anzeige nach § 14 Kreditwesen-Gesetz) wurden durch Erläuterungen des Bundesministers der Finanzen ausgeräumt; über die übrigen Verbesserungsvorschläge wurde einvernehmlich entschieden.

Offen ist noch die Verwendung des sogenannten Verbundformulars für die Meldung nach § 59 Außenwirtschaftsverordnung (AWV). Ich hatte darauf hingewiesen, daß damit sowohl geschäftliche als auch statistische Daten unnötigerweise allen Beteiligten mitgeteilt werden. Der Bundesminister für Wirtschaft und die Bundesbank anerkennen meine Bedenken. Die Verhandlungen mit der Kreditwirtschaft mit dem Ziel einer drucktechnischen Änderung des Formularsatzes haben zu keiner Übereinkunft geführt. Die Bundesbank hat nunmehr eine Änderung der Außenwirtschaftsverordnung vorgeschlagen, um — entsprechend meinen Vorschlägen — dem Betroffenen die Abgabe getrennter Erklärungen zu ermöglichen.

Für den Geschäftsbereich der Deutschen Bundesbank war zu klären, ob die im Zusammenhang mit Zahlungen nach dem Unterhaltssicherungsgesetz (USG) bestehenden Sicherungsvorkehrungen ausreichend sind. Bedenken gegen die dabei geübte Praxis des Datenträgeraustausches wurden von einer Gemeinde angemeldet. Als zusätzliche Sicherungsmaßnahme forderte sie von der Landeszentralbank, die eingereichten Datenträger vor dem Rücktransport zu löschen, ersatzweise sie als Wertpaket zurückzusenden.

Meine Prüfung ergab, daß für diesen Vorgang eine hinreichende Datensicherung besteht. So ist beispielsweise sichergestellt, daß Magnetbänder nur dem jeweiligen Einreicher zurückgegeben werden, d. h. unbefugte Dritte keine Kenntnis erhalten; die einzelnen Datensätze enthalten keine vollständigen Adreßangaben, sondern lediglich Name und Kontonummer des Betroffenen, so daß die Identifizierung wesentlich erschwert ist; der Verwendungszweck wird abgekürzt (z. B. Leistung gemäß USG 9/82). Da auf dem Bankbeleg keine weiteren Angaben erfolgen und die Zahl der Leistungsempfänger sehr groß ist, führen die vorhandenen Informationen nur unter größeren Anstrengungen zu einer Bestimmbarkeit von Betroffenen. Für unbefugte Dritte müßten solche Anstrengungen durch entsprechende Vorteile ausgeglichen werden. Dafür gibt es jedoch keine Anhaltspunkte. Das Risiko einer Beeinträchtigung schutzwürdiger Belange ist daher sehr gering.

Da sich der Sicherungsaufwand am Schutzbedürfnis orientiert (§ 6 BDSG), habe ich der Deutschen Bundesbank bestätigt, daß keine zusätzlichen Si-

cherungsmaßnahmen zur Verringerung des Transportrisikos geboten sind.

Der erwähnten Gemeinde konnte alternativ zum praktizierten Datenträgeraustauschverfahren vorgeschlagen werden, die ohnehin bestehenden Kurierdienste zu benutzen.

2.17.4 Öffentlich-rechtliche Banken

Von den der Aufsicht des Bundes unterliegenden öffentlich-rechtlichen Banken habe ich die Deutsche Siedlungs- und Landesrentenbank (DSL-Bank), die Lastenausgleichsbank (LAB) und die Kreditanstalt für Wiederaufbau (KfW) datenschutzrechtlich überprüft.

Konkrete Einzelbeschwerden über den Umgang mit personenbezogenen Daten hat es aus diesem Bereich nicht gegeben. Aufgrund der Prüfungserfahrung kann ich feststellen, daß die Verarbeitung personenbezogener Daten im großen und ganzen mit Sorgfalt durchgeführt wird. Dies liegt wesentlich daran, daß die Datenverarbeitung in vielen Fällen mit Zahlungsvorgängen verbunden ist und die Banken deshalb schon im eigenen Interesse auf genaue Prüfungen und hohe Sicherheitsstandards großen Wert legen. Zudem sehen sie ihren Ruf eng mit der strikten Beachtung des Bankgeheimnisses verknüpft.

Bei einigen regelmäßig praktizierten Informationsvorgängen habe ich dennoch datenschutzrechtliche Bedenken anmelden müssen. Sie richten sich gegen die Speicherung bestimmter Daten, in anderen Fällen gegen Datenübermittlungen. Außerdem war mehrfach die unzureichende Aufklärung der Betroffenen über die mit dem Kreditgeschäft zusammenhängende Datenverarbeitung zu monieren.

Die Datenschutzregelungen für öffentliche Unternehmen, die am Wettbewerb teilnehmen, sind im 3. Abschnitt des BDSG festgelegt und orientieren sich an den zwischen den Parteien angebahnten bzw. bestehenden Vertragsverhältnissen (§§ 23 ff. BDSG). Die Verarbeitung personenbezogener Daten ist danach zulässig, soweit sie „im Rahmen" der geschäftlichen Beziehungen liegt; d. h. objektiver Anknüpfungspunkt ist der Zweck des Vertragsverhältnisses.

Folgende Beispiele mögen dies verdeutlichen:

a) Über die Vermittler von Verträgen war eine Datei angelegt, in der u. a. Beurteilungen der Vermittler sowie der Geschäftsbeziehungen mit ihnen anhand von fünf vorgegebenen Kategorien (von „sehr positiv" bis „sehr negativ") erfolgte.

   Ich habe darauf hingewiesen, daß die Einschätzungen anhand der Beurteilungskategorien sehr subjektiv erfolgen, die Ableitung aus bestimmten Tatsachen nicht nachvollziehbar ist und die Bewertungsgrundsätze nicht erkennbar sind. Außerdem war auf die fehlende Transparenz dieser Datei hinzuweisen. Es war nicht davon auszugehen, daß den Betroffenen eine solche Datenspeicherung bekannt war, so daß sie nach § 26 Abs. 1 BDSG hätten benachrichtigt werden müssen.

   Gegen das Bedürfnis der Banken, sich über ihre Geschäftspartner ins Bild zu setzen, ist selbstverständlich nichts einzuwenden. Es war jedoch zu prüfen, ob die zu speichernden Daten — hier die Beurteilungsmerkmale — geeignet sind, die tatsächlichen Verhältnisse widerzuspiegeln.

   Meinen Bedenken hat das Institut Rechnung getragen und die Datei gelöscht.

b) Bei der Entgegennahme von Subventionsanträgen werden vom Antragsteller auf einem gesonderten Vordruck „ergänzende statistische Angaben" erhoben. Dazu erfolgt auf dem Antragsvordruck der Hinweis, daß die zusätzlich erbetenen Informationen „erforderlich" seien.

   Ich habe keine grundsätzlichen datenschutzrechtlichen Bedenken gegen die Erhebung und Auswertung ergänzender, also die Subventionsbewilligung nicht beeinflussender Daten, solange diese für die sachgerechte Abwicklung oder die Evaluierung des Programms erforderlich sind und ihre Erhebung nicht unverhältnismäßig in die Privatsphäre des Betroffenen eingreift. Dienen die ergänzenden Angaben der Subventionsentscheidung — und dafür spricht der Hinweis auf die „Erforderlichkeit" im Antragsvordruck —, dann darf der Vordruck nicht als „Statistisches Beiblatt" überschrieben sein. Werden die Daten allerdings nicht zur Evaluierung des konkreten Förderungsprogramms, sondern für weitergehende statistische Zwecke erhoben, dann wäre auf die Freiwilligkeit der Beantwortung hinzuweisen. Eine Auskunftspflicht könnte nur durch Gesetz begründet werden.

   Im vorliegenden Fall hat die Bank in ihrer Stellungnahme betont, daß es sich um entscheidungsrelevante Daten handele. Da das Subventionsprogramm bereits ausgelaufen ist, war eine Korrektur nicht mehr möglich. In künftig auftretenden gleichartigen Fällen wird die Bank meiner Empfehlung folgen und den Vordruck deutlich entweder als Teil des Antrags oder als statistisches Beiblatt mit freiwilliger Beantwortung kennzeichnen.

c) Kopien der Erfassungsbögen für Investitionskredite wurden regelmäßig einem Bundesamt „zur regionalen statistischen Auswertung" überlassen. Diese Datenübermittlung in nicht anonymisierter Form war weder durch eine besondere Rechtsvorschrift noch durch die Einwilligung des Betroffenen gedeckt. Sie konnte — jedenfalls mit voller Angabe von Namen und Anschrift — auch nicht auf § 24 Abs. 1 BDSG gestützt werden, da die Weitergabe von identifizierenden Angaben nicht im Rahmen der Zweckbestimmung des Vertragsverhältnisses liegt und auch nicht zur Wahrnehmung berechtigter Interessen des Bundesamtes oder der Allgemeinheit erforderlich ist.

   Die Weitergabe in personenbezogener Form wurde eingestellt.

d) In meinem letzten Tätigkeitsbericht hatte ich über die Erteilung von Bankauskünften berichtet (vgl. 4. TB S. 40).

Die Berechtigung zu Bankauskünften leitet die Kreditwirtschaft aus der Notwendigkeit ab, sich über die wirtschaftlichen Verhältnisse ihrer Kreditnehmer zu erkundigen. Da es sich um einen branchenüblichen Informationsaustausch handelt, geht die Kreditwirtschaft davon aus, daß die Datenübermittlungen „im Rahmen" der Zweckbestimmung des Vertragsverhältnisses liegen und somit datenschutzrechtlich unbedenklich sind.

Meine datenschutzrechtlichen Bedenken richten sich nicht gegen eine sachgerechte Bonitätsprüfung, sondern in erster Linie gegen die in der Praxis vorgenommenen vagen und für Kreditentscheidungen kaum verwertbaren Persönlichkeitsbeurteilungen. Darüber hinaus habe ich Bedenken, ob sich Bankauskünfte mit dem Hinweis auf die üblichen Geschäftspraktiken der Kreditwirtschaft begründen lassen. Wenn ein Informationsvorgang sich „im Rahmen" des Geschäftsüblichen bewegen soll, dann müssen diese Geschäftsusancen auch der anderen Vertragsseite, d. h. hier den Betroffenen, bekannt sein. Solange es aber an der Transparenz fehlt bzw. solange in den Finanzierungsbedingungen nur unzureichend aufgeklärt wird (z. B.: „Gläubiger des Darlehensnehmers ... sind ermächtigt ... der ... Bank alle Auskünfte zu geben ..."), liegt die Übermittlung nach meiner Auffassung nicht im Rahmen der Zweckbestimmung des Vertragsverhältnisses; sie könnte nur durch die Einwilligung des Betroffenen gerechtfertigt werden.

Die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sind mit mir der Ansicht, daß die Voraussetzungen für ein datenschutzrechtlich unbedenkliches Verfahren derzeit nicht gegeben sind. Durch gemeinsame Verhandlungen mit den entsprechenden Wirtschaftsverbänden soll eine einheitliche, datenschutzgerechte Lösung erreicht werden.

2.17.5 Versicherungen

Versicherungsunternehmen sind ganz überwiegend privatrechtlich, in einigen Fällen aber auch öffentlich-rechtlich organisiert. Darunter sind auch zwei Stellen des Bundes. Da es nur wenige Beschwerden Betroffener gab, lag der Schwerpunkt meiner Tätigkeit in der Prüfung, ob die in den Versicherungsbedingungen enthaltenen Erklärungen zum Datenschutz den Anforderungen des BDSG genügen. Gemeinsam mit dem Bundesaufsichtsamt für das Versicherungswesen, dem prinzipiell alle Versicherungsbedingungen zur Genehmigung vorzulegen sind, den Aufsichtsbehörden für die Datenschutzkontrolle im nicht-öffentlichen Bereich und der Versicherungswirtschaft habe ich an den Beratungen zur Neugestaltung der Klausel mitgewirkt.

Die ursprünglich verwendete sogenannte Datenschutzklausel war in der Formulierung inhaltlich zu unbestimmt und für den Betroffenen nicht verständlich genug (vgl. 1. TB S. 41). In den Verhandlungen wurde der Versuch unternommen, Zweck, Art und Umfang der Übermittlungstatbestände, die von der Klausel betroffen sind, klarer als bisher herauszustellen und die Klausel allgemein verständlicher zu fassen (vgl. 2. TB S. 55).

Die überarbeitete und abgestimmte Klausel wird seit 1981 in den Vordrucken der Versicherungsbranche verwendet. Darüber hinaus wurde ein Merkblatt mit zusätzlichen Erläuterungen zu den Datenverarbeitungsvorgängen in den einzelnen Versicherungssparten erarbeitet, das der Betroffene von seiner Versicherung anfordern kann. Auf dieses Angebot wird formularmäßig hingewiesen. Gegenüber dem Bundesaufsichtsamt haben sich die Versicherer durch geschäftsplanmäßige Erklärungen zu einem bestimmten aufklärenden Verhalten in Beschwerdefällen verpflichtet.

Nachdem diese Regelungen seit nunmehr zwei Jahren wirken, erreichen mich nur noch einzelne Petitionen. Dies werte ich als ein gutes Zeichen für die entwickelte Kompromißlösung.

Aber auch in den verbliebenen Beschwerdefällen ist mir kein Vorgang bekannt geworden, bei dem ein Versicherer — gestützt auf die unterschriebene Klausel — unzulässige Datenübermittlungen vorgenommen hätte.

Neben der sogenannten Datenschutzklausel wird beim Abschluß von Kranken- und Lebensversicherungsverträgen vom Versicherungsnehmer routinemäßig eine Entbindung von der ärztlichen Schweigepflicht gefordert. Diese „Schweigepflichtentbindungsklausel" soll es den Versicherern ermöglichen, die Angaben des Betroffenen zur tarifmäßigen Einstufung sowie im Versicherungsfall den Umfang der Leistungspflicht zu überprüfen. Dadurch können unberechtigte Forderungen abgewehrt werden.

Die Formulierung dieser Klausel begegnet ähnlichen Bedenken wie die der ursprünglichen „Datenschutzklausel". Auch hier sind Einschränkungen und Präzisierungen erforderlich. Die Datenschutzaufsichtsinstanzen haben die Problematik aufgegriffen und streben eine Abstimmung mit der Versicherungswirtschaft an. Zur Zeit werden die einzelnen Problempunkte herausgearbeitet. Dazu gehören beispielsweise die Fragen, in welchem Umfang die von der Schweigepflicht entbundenen Personen und Stellen zur Auskunft ermächtigt und ob sie dazu auch verpflichtet sind, wie die auskunftgebende Stelle zu prüfen hat, ob eine wirksame Entbindung von der Schweigepflicht tatsächlich vorliegt, und wie zu verfahren ist, wenn Zweifel bestehen, ob die gewünschte Information durch den Inhalt der Klausel gedeckt ist.

3 Öffentliche Sicherheit und Verteidigung

3.1 Überblick

3.1.1 Die Kontrolltätigkeit und ihr Niederschlag in diesem Bericht

In diesem Jahr wurde die systematische Prüfung und Beratung bei verschiedenen Sicherheitsbehörden fortgesetzt. Nach den umfangreichen Kontrollen, die ich im Jahre 1981 beim Bundeskriminalamt und beim Bundesamt für Verfassungsschutz zum jeweiligen Bereich Terrorismus habe durchführen lassen, waren nunmehr Schwerpunkte der datenschutzrechtlichen Kontrolle:

— die Abteilung Staatsschutz des Bundeskriminalamts und die Tätigkeit des BKA als Nationales Zentralbüro von INTERPOL,

— die Datenverarbeitung des Militärischen Abschirmdienstes sowie

— verschiedene Teilbereiche der Datenverarbeitung des Bundesnachrichtendienstes.

Außerdem wurde mit einer behördenübergreifenden Prüfung begonnen, ob die neue Regelung zur Amtshilfe des Bundesgrenzschutzes für die Nachrichtendienste beachtet wird und welche Auswirkungen sie hat. Daneben waren wieder zahlreiche Einzelangaben zu bearbeiten; manche von ihnen lieferten wertvolle Hinweise zur Klärung grundsätzlicher Fragen.

Ziel der folgenden Darstellung ist es, die Entwicklung der Informationsverarbeitung im Sicherheitsbereich deutlich zu machen sowie die gelösten und die verbleibenden Probleme zu benennen. Es ist nicht möglich, in einem Tätigkeitsbericht, der nicht unverhältnismäßig lang ausfallen soll, eine vollständige Darstellung von Stand und Entwicklung der Datenverarbeitung und des Datenschutzes bei den Sicherheitsbehörden zu geben. Zwischen den einzelnen Stellen bestehen auch erhebliche Unterschiede.

Die durchgeführten Prüfungen haben — wie in den vergangenen Jahren — zu einer Vielzahl von Empfehlungen, aber auch wieder zu einer Reihe von Beanstandungen geführt. Die betreffenden Behörden haben die Berechtigung meiner Beanstandungen im wesentlichen bereits anerkannt und die Löschung kritisierter Speicherungen in Angriff genommen.

Dies gilt übrigens auch für die meisten der im Jahre 1981 ausgesprochenen und im Vierten Tätigkeitsbericht (S. 21 ff.) dargestellten Beanstandungen. Die Prüfungen des vergangenen Jahres haben andererseits eine Reihe ermutigender Beispiele für bemerkenswerte datenschutzrechtliche Fortschritte erbracht.

In diesem Jahr hat die Berichterstattung über das Bundeskriminalamt einen beträchtlichen Anteil am Gesamtumfang dieses Berichts, während andere Behörden ralativ knapp abgehandelt werden. Das liegt zum einen daran, daß ich 1982 beim BKA zwei auf längere Zeit angelegte, systematische Prüfungen durchgeführt habe. Andererseits sind gerade in diesem Jahr beim BKA eine Reihe neuer Dateien errichtet worden, die im Bericht angesprochen werden müssen. Wenn also Probleme im Bereich des BKA in diesem Tätigkeitsbericht Übergewicht haben, so heißt dies nicht, daß gerade dieses Amt ganz besonderen Grund zu datenschutzrechtlicher Kritik gäbe. Im nächsten Jahr können sich wieder andere Schwerpunkte ergeben.

Versucht man die Feststellungen bei den einzelnen Sicherheitsbehörden auf einen gemeinsamen Nenner zu bringen, so wäre es sicher falsch, die Situation zu beschönigen und die bestehenden Bedenken zu verdrängen. Das Datenschutzrecht ist bei den Sicherheitsbehörden noch nicht voll verwirklicht. Daraus „Abgründe von Rechtswidrigkeit" ersehen zu wollen, ginge jedoch ebenso an den Tatsachen vorbei. Fehler bei der Datenverarbeitung werden in allen Bereichen gemacht; die Sicherheitsbehörden sind davon nicht verschont geblieben. Meine Mitarbeiter mußten einmal sogar feststellen, daß ein rechtskräftiges Urteil auf Löschung aller Daten einer Person in den Dateien einer Sicherheitsbehörde nach fast zwei Jahren noch nicht vollzogen war — offensichtlich keine Mißachtung des Gerichts, sondern Nachlässigkeit (der Fall wurde auf unser Tätigwerden hin inzwischen erledigt). Man muß auch berücksichtigen, daß die vollständige Vollziehung des Datenschutzrechts von den Sicherheitsbehörden besonders viel Aufwand erfordert. Umfangreiche Bereinigungsarbeiten sind allenthalben in Gang gekommen.

Insgesamt sind in den vergangenen fünf Jahren spürbare Verbesserungen auf vielen Gebieten der Datenverarbeitung bei den Sicherheitsbehörden erreicht worden. Da aber gleichzeitig die Nutzung der Informationstechnik gerade in diesem Bereich wesentlich erweitert wurde und künftig noch weiter ausgebaut werden soll, besteht kein Grund, in den Bemühungen um die Verwirklichung von Datenschutz nachzulassen.

3.1.2 Quellenschutz

Nach § 19 Abs. 3 Satz 4 des BDSG kann im Bereich der Sicherheitsbehörden die zuständige oberste Bundesbehörde im Einzelfall feststellen, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet; die entsprechenden Unterlagen brauchen mir nicht vorgelegt zu werden. Es handelt sich hierbei um eine

Ausnahmevorschrift, die in der Praxis so gut wie keine Rolle spielt. In den Unterlagen der Sicherheitsbehörden, insbesondere der Nachrichtendienste, finden sich bisweilen die Berichte verdeckter Mitarbeiter, die dann mit dem Vermerk „Quellenschutz" versehen sind. Es dürfte in aller Regel nicht die Sicherheit des Bundes oder eines Landes gefährden, wenn ich oder meine speziell beauftragten Mitarbeiter die Identität derartiger V-Leute erfahren. Andererseits erfordert meine Kontrolltätigkeit nicht unbedingt die Einsicht in derartige Unterlagen. Ich habe deshalb meine bisherige Prüftätigkeit bei den Sicherheitsbehörden stets so ausgeübt, daß weder meine Mitarbeiter noch ich Kenntnis von der Identität geheimer Mitarbeiter genommen haben. Die Qualität meiner Kontrolle wurde dadurch nicht beeinträchtigt, während andererseits dem Interesse der Sicherheitsbehörden und ihrer verdeckten Mitarbeiter an der Geheimhaltung ihrer Identität auch vor mir Rechnung getragen wurde. Dies soll auch künftig so bleiben.

3.1.3 Einschränkung meiner Kontrolltätigkeit durch das BfV

Im November des vergangenen Jahres hat das Bundesamt für Verfassungsschutz während einer laufenden Prüfung erstmals eine neue Definition meiner Prüfbefugnis zur Anwendung gebracht, die eine Fortsetzung meiner Prüftätigkeit unmöglich machte. Das Bundesamt für Verfassungsschutz speichert ebenso wie die Landesämter für Verfassungsschutz im System NADIS Personendaten und die dazugehörigen Aktenfundstellen. Die Rechtfertigung für die Registrierung einer Person kann sich nur aus den Aktenfundstellen ergeben. Bislang habe ich die Berechtigung einer Speicherung immer im Wege der Durchsicht dieser Aktenfundstellen überprüft. Maßstab der Beurteilung war die Gesamtheit der in der Akte enthaltenen Informationen, also auch entlastende Tatsachen. Nicht selten lautete dabei das Ergebnis auch so, daß gegen die Speicherung als solche nichts einzuwenden war, wohl aber gegen einzelne Schritte der Datenverarbeitung, z. B. gegen die Übermittlung von Informationen an andere Behörden. Da ich von der Vielzahl der beim Verfassungsschutz gespeicherten Akten schon aus Kapazitätsmangel immer nur einen verschwindend geringen Prozentsatz überprüfen kann, habe ich immer versucht, aus der Prüfung der Einzelfälle allgemeine Erkenntnisse zu gewinnen und Aussagen auch zu allen gleichgelagerten Fällen zu machen. Wenn man bedenkt, daß mir für die Kontrolle aller Sicherheitsbehörden des Bundes nur vier Mitarbeiter zur Verfügung stehen, so wird man einräumen müssen, daß nur mit Hilfe allgemeiner Querschnittsprüfungen und -Analysen die zu prüfende Aktenmenge auch nur annähernd bewältigt werden kann.

Auch die Landesbeauftragten für den Datenschutz haben ausdrücklich betont, daß ihre Prüfbefugnis auch das Recht zur vollständigen Einsicht in gespeicherte Akten umfaßt.

Im August dieses Jahres habe ich begonnen, Fälle aus dem Bereich der Amtshilfe des BGS für das BfV nachzuprüfen. Aus technischen Gründen konnte die Prüfung erst im November fortgesetzt werden. Nunmehr stellte sich das BfV auf den Standpunkt, es sei nicht schon dann verpflichtet, mir Einsicht in Akten zu geben, wenn sie in NADIS zu einer Person registriert sind. Vielmehr sei jeweils zu prüfen, ob der Kontrollzweck bei einer teilweisen Einsicht nicht unter Umständen bereits erreicht werde und/oder ob die Einsicht in weitere Teile, gegebenenfalls auch in den *vollständigen* Inhalt der betreffenden Akte (noch) erforderlich sei. Um etwa die Frage zu beantworten, ob eine Person zu Recht in NADIS gespeichert sei, genüge es, nur diejenigen Teile bzw. Seiten der Akte zu zeigen, die nötig seien, damit ich beurteilen könne, ob ein entsprechender Verdacht vorliege oder nicht.

Ich habe mich unter diesen Umständen nicht in der Lage gesehen, die beabsichtigte Prüfung durchzuführen. Zu einer Kontrolle gehört nach meiner Auffassung, daß der Prüfer sich selbst anhand der gesamten Akte ein vollständiges Bild machen kann. Davon kann nach meiner Auffassung nicht mehr gesprochen werden, wenn der Geprüfte sich die Entscheidung vorbehält, welche Unterlagen er vorlegt und welche nicht. Der Prüfer hat dann nicht mehr die Sicherheit, sich von den Tatsachen selbst zu überzeugen. Um dies am Beispiel deutlich werden zu lassen: Die Seiten 15 bis 20 einer Akte mögen eindeutig den Verdacht ergeben, daß eine Person ein Träger extremistischer Bestrebungen ist, während auf S. 21 dieser Verdacht entkräftet wird. Ob Daten über eine Person übermittelt worden sind, läßt sich nur durch das Studium der gesamten Akte erklären.

Querschnittsprüfungen sind nur bei vollständiger Auswertung repräsentativer Akten möglich. § 19 Abs. 3 Satz 2 Nr. 1 BDSG verpflichtet das BfV, mir und den von mir Beauftragten Einsicht in alle Unterlagen und Akten zu geben, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Nach § 19 Abs. 3 Satz 1 ist das BfV verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen.

Nach meiner Ansicht hat deshalb das BfV in Widerspruch zum Gesetz gehandelt, als es die unbeschränkte Einsicht in die Akten verweigerte, die zu einer Person gespeichert waren.

Der Innenausschuß des Deutschen Bundestages hat sich in seinen Sitzungen am 2. und 8. Dezember mit dem Problem befaßt. Ich habe im Innenausschuß erklärt, daß ich auf der Basis des vom BfV vorgeschlagenen Verfahrens keine datenschutzrechtlichen Kontrollen beim BfV mehr durchführen kann. Der Vorsitzende des Innenausschusses hat im Laufe der Sitzung den BMI und mich aufgefordert, nach einer Lösung zu suchen, die die Fortsetzung meiner Prüftätigkeit möglich macht. Ich habe mich daraufhin in Absprache mit dem BMI damit einverstanden erklärt, daß bei der Fortsetzung meiner Prüftätigkeit ein Vertreter des BMI anwesend ist, der auftretende Zweifelsfragen an Ort und Stelle „in Orientierung an der bisherigen Prüfpraxis" klärt. Zugleich habe ich im Innenausschuß zum Ausdruck gebracht, daß ich davon ausgehe, daß mit

dieser Regelung eine ungehinderte Fortsetzung meiner Prüftätigkeit im bisherigen Umfang möglich sei. Der BMI hat erklärt, daß er die vom BfV aufgeworfenen Fragen in Abstimmung mit den anderen Ressorts und den Ländern grundsätzlich klären will, da das Problem der Akteneinsicht nicht nur die Sicherheitsbehörden, sondern alle Stellen betreffe, deren Akten durch automatisierte Dateien erschlossen werden. Er gehe davon aus, daß diese Prüfung bis Ende Februar 1983 abgeschlossen sei. Die jetzt gefundene Regelung solle bis dahin gelten und die zu treffende Grundsatzentscheidung nicht präjudizieren.

Am 22. Dezember 1982 habe ich dann die unterbrochene Prüfung fortsetzen lassen. Ein Vertreter des BMI hat daran nicht teilgenommen. Zur Klärung auftretender Zweifelsfragen hielten sich jedoch die zuständigen Beamten des BMI bereit. Das BfV hat eingangs der Prüfung seinen unveränderten Standpunkt deutlich gemacht und angeboten, jeweils an Hand der einzelnen Akte zu erläutern, welche Akteile für den bekanntgegebenen Prüfungszweck relevant/irrelevant erscheinen. Meine Mitarbeiter haben darauf entgegnet, sie wollten sich selbst ein Bild von der Relevanz/Irrelevanz der Akten machen. Daraufhin hat das BfV, so wie es auch bisher Prüfungspraxis war, die Akten mit Ausnahme von Quellenschutzteilen (siehe oben 3.1.2) in vollem Umfang vorgelegt. Die Prüfung konnte dann in dem Umfang ohne Behinderung fortgesetzt werden, in dem sie im August begonnen worden war.

Ich hoffe, daß die aufgetretenen Streitfragen damit fürs erste geklärt sind, und erwarte wegen der nach meiner Ansicht eindeutigen Gesetzeslage, daß auch die endgültige Klärung durch den BMI im Februar 1983 zu keinem anderen Ergebnis führen wird.

3.2 Gemeinsame Probleme

Bei allen Sicherheitsbehörden gibt es gemeinsame Probleme:

— Umfang der Speicherung, insbesondere Abgrenzung der Aufgabengebiete (3.2.1)

— Zulässigkeit der Übermittlung an andere Behörden (Amtshilfe); damit verbunden sind Fragen der Datengenauigkeit und der Nachberichterstattung (3.2.2)

— Überprüfungs- und Löschungsfristen, Behandlung der „Altfälle" (3.2.3)

— Auskunftsverhalten gegenüber dem Bürger (3.2.4).

Besonders im Polizeibereich ist die Bewältigung dieser Fragen dringend. Denn hier werden die meisten Informationen gespeichert und untereinander ausgetauscht. Als übergreifendes Thema ist auch das Verfahren der Dateianfrage (4. TB S. 29) nochmals anzusprechen (s. unten 3.2.5).

3.2.1 Zum Umfang der Speicherung

Die Speicherung im polizeilichen Bereich hat häufig und in steigendem Maße, im nachrichtendienstlichen Bereich in überwiegendem Maße den Zweck, Unterlagen bereitzuhalten, aus denen sich bei späteren Ereignissen Schlüsse auf sonst nicht bekanntwerdende Zusammenhänge ziehen lassen. Verkürzt ausgedrückt, dienen viele Speicherungen der „Verdachtsverdichtung". Ausnahmen sind im nachrichtendienstlichen Bereich z. B. die Registrierungen, die im Zusammenhang mit der Sicherheitsüberprüfung oder nur zu reinen Verwaltungszwecken vorgenommen werden (solange eben dieser Verwendungszweck eingehalten wird!). Im polizeilichen Bereich dient z. B. die Fahndungsnotierung überwiegend der Festnahme oder Aufenthaltsermittlung.

Fehlte es aber bei genauer Betrachtung an hinreichenden Anhaltspunkten für einen Anfangsverdacht oder waren die festgestellten Anhaltspunkte nicht stichhaltig, so bewirkt eine dennoch vorgenommene oder aufrechterhaltene Speicherung, daß die Betroffenen ungerechtfertigten Verdächtigungen, belastenden Ermittlungen und im ungünstigsten Fall sogar diskriminierenden Verfahren ausgesetzt werden. Diese Gefahr für das Interesse des einzelnen, nicht ohne Grund mit belastenden staatlichen Maßnahmen behelligt zu werden, erhöht sich noch wesentlich, wenn über solche Unterlagen — wie nicht selten — Auskünfte an dritte Stellen erteilt werden. Auch die Eröffnung der Möglichkeit zur Direktabfrage durch andere Stellen als die sachbearbeitende Polizeibehörde erhöht diese Gefahr. Je mehr ungesicherte Daten die Polizei oder die Nachrichtendienste speichern, desto geringer wird übrigens auch deren Nutzen für die eigene Arbeit dieser Behörden.

Daß nach wie vor mehr Daten gespeichert werden als unbedingt erforderlich, liegt zum Teil am Fehlen bzw. an der generalklauselhaften Form der rechtlichen Regelungen. So ist die Tätigkeit der Nachrichtendienste überwiegend gar nicht rechtlich geregelt. Auch die innerdienstlichen Vorschriften sind zum Teil recht weit gefaßt. Für das BKA enthält Nr. 4. 1.11 der Dateien-Richtlinien die Erlaubnis, auch Daten „anderer Personen" zu speichern, die weder Beschuldigte noch Verdächtige noch (im polizeirechtlichen Sinne) Störer sind, bei denen aber „zureichende Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Straftaten, zur Ergreifung oder zur Festnahme gesuchter Personen oder zur Abwehr einer im einzelnen Fall bestehenden erheblichen Gefahr erforderlich ist". Eine solche Registrierung von Personen, bei denen man eben noch nicht weiß, ob sie einmal zu Verdächtigen oder Beschuldigten werden oder als Zeugen in Betracht kommen, ist im Strafverfahrensrecht nicht vorgesehen und kann auch nach Polizeirecht nur unter engen Voraussetzungen gerechtfertigt werden. Wenn jemand nämlich weder Verdächtigter noch Beschuldigter ist, aber gleichwohl seine Notierung z. B. etwas zur Ergreifung von gesuchten Personen beitragen kann, so hat er nach üblichem Sprachgebrauch die Stellung eines Zeugen oder Hinweisgebers. Zeugen und Hinweisgeber dürfen nach den Dateienrichtlinien nur in zeitlich befristet geführten Spurendokumentationssystemen gespeichert werden. Die PIOS-Systeme sind aber auf

Dauer angelegt. Wenn in den Dateienrichtlinien im Gegensatz dazu die Speicherung „anderer Personen“ unter bestimmten Voraussetzungen für zulässig erklärt worden ist, so ging man offenbar von der Annahme aus, es gebe zwischen Zeugen, Hinweisgebern und Verdächtigen noch eine Zwischenstufe, eben die „anderen Personen“. Ich vermag diese Unterscheidung nur schwer nachzuvollziehen.

Hierauf habe ich gemeinsam mit den Datenschutzbeauftragten der Länder vor Verabschiedung der Dateien-Richtlinien hingewiesen — leider vergeblich. Die Richtlinien enthalten zwar die Bestimmung, daß die in Nummer 4.2.11 umschriebenen „anderen Personen“ über die Tatsache der Speicherung zu unterrichten sind, sobald die Dauer der Speicherung ein Jahr überschritten hat. Nach den Feststellungen über die Datei PIOS-Terrorismus, die meine Mitarbeiter im Jahre 1981 getroffen haben, wurde aber von der Speicherungserlaubnis recht weitgehend Gebrauch gemacht, die Unterrichtung unterblieb jedoch in den meisten Fällen, weil das BKA davon ausging, daß durch sie der mit der Speicherung verfolgte Zweck gefährdet würde (Nr. 4.5.2 der Dateien-Richtlinien; vgl. 4. TB S. 23). Leider enthält die überwiegende Anzahl der in letzter Zeit festgelegten Errichtungsanordnungen für neue Dateien im BKA ebenfalls den Begriff der „anderen Personen“ bei der Umschreibung des Personenkreises, über den Daten gespeichert werden dürfen (vgl. dazu auch unten Nr. 3.3.1).

Manche Rechtsvorschriften werden zu extensiv ausgelegt. So haben Prüfungen ergeben, daß nicht selten erkennungsdienstliche Unterlagen gespeichert wurden, obwohl die gesetzlichen Voraussetzungen, die dies in jenen Fällen hätten rechtfertigen können (Verdacht auf Vorliegen einer bedeutenderen Straftat und Anhaltspunkte für Wiederholungsgefahr), nicht mit hinreichender Deutlichkeit erkennbar waren. Ein weiterer Grund für zu umfangreiche Speicherung liegt darin, daß die Erforderlichkeit nicht streng genug geprüft wird. So finden, wie den jeweiligen Behördenverteilern zu entnehmen ist, rein „nachrichtliche“ Unterrichtungen nach wie vor in recht großem Umfang statt. Dies kann Empfänger zu unnötigen Speicherungen verführen.

Andererseits muß betont werden, daß bei allen Sicherheitsbehörden des Bundes das Problembewußtsein wächst und zunehmend Ansätze erkennbar sind, nicht nur unnötige Sammlungen von Altfällen (dazu unten Nr. 3.2.3) abzubauen, sondern neue nicht erforderliche Speicherungen von vornherein zu vermeiden.

3.2.2 Zulässigkeit der Übermittlung an andere Behörden (Amtshilfe)

Es ist nicht selbstverständlich, daß Daten, die eine Behörde rechtmäßig für ihre Zwecke gespeichert hat, auch anderen Behörden übermittelt werden dürfen.

So hatte ich im vergangenen Jahr aufgrund mehrerer Eingaben der Frage nachzugehen, ob es rechtmäßig ist, wenn die Bahnpolizei die Namen der Verteiler von Flugblättern zum Thema „Kriegsdienstverweigerung“ an Feldjäger der Bundeswehr oder an den MAD weitergibt. MAD und Feldjäger selbst sind nicht befugt, Privatpersonen anzuhalten und die Personalien festzustellen. Auf dem Umweg über die Amtshilfe der Bahnpolizei ist dies aber zumindest mittelbar geschehen. Ich halte dies nicht für zulässig.

Zwar erlaubt § 10 BDSG die Übermittlung auch zur Aufgabenerfüllung der empfangenden Stelle; soweit aber in der Übermittlung eine zusätzliche Belastung der Betroffenen liegt, bedarf sie ihrerseits der gesetzlichen Ermächtigung — dies ist im Sicherheitsbereich regelmäßig der Fall. Übermittlungsermächtigungen enthalten Vorschriften wie §§ 2 bis 4 Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamtes) (BKAG), 7 Abs. 3 Gesetz zu Artikel 10 Grundgesetz, 4 Abs. 1 Gesetz über die Zusammenarbeit des Bundes und der Länder und Angelegenheiten des Verfassungsschutzes. Damit sind der polizeiliche und der nachrichtendienstliche Informationsverbund — je für sich — rechtlich weitgehend abgesichert. Die speichernden Stellen sind aber auch in diesen Fällen verpflichtet, jeweils die Erforderlichkeit der Übermittlung sorgfältig zu prüfen. Nur in seltenen, gesetzlich im einzelnen umschriebenen Fällen wie nach § 138 Strafgesetzbuch ist der „Herr der Daten“ der Abwägungspflicht enthoben, weil der Gesetzgeber hier, um besonders schwere Gefahren abzuwehren, eine Pflicht zur Übermittlung bestimmt hat. Bedenklich ist aber — wie ich schon mehrfach ausgeführt habe — der bisher praktizierte Informationsverbund zwischen Polizei und Nachrichtendiensten. Damit ist das überlicherweise unter dem Stichwort „Amtshilfe“ behandelte Thema angesprochen. Hierauf bin ich in meinen früheren Tätigkeitsberichten schon mehrfach eingegangen. Die Meinungsverschiedenheiten darüber, inwieweit das allgemeine Amtshilfegebot (Artikel 35 GG) Übermittlungen personenbezogener Daten gegenüber dem Betroffenen rechtfertigt, dauern an. Noch so differenzierte und ausgewogene Regelungen für die Speicherung von Daten bei einer Sicherheitsbehörde verlieren aber deutlich an Wert, wenn die Daten allein aufgrund des Amtshilfegebotes an andere Sicherheitsbehörden mit möglicherweise ganz anderen Datenverarbeitungsvorschriften übermittelt werden.

In meinem letzten Tätigkeitsbericht hatte ich einige Formen der Amtshilfe zwischen BKA und BfV kritisch beleuchtet, soweit sie die Verarbeitung personenbezogener Daten betreffen. Insbesondere die Beschlüsse der IMK aus dem Jahre 1977 über die Zusammenarbeit im Bereich der Terrorismusbekämpfung stehen nach meiner Ansicht nicht alle im Einklang mit dem verfassungskräftigen Gebot der Trennung von Polizei und Verfassungsschutz. Ich habe dem Bundesminister des Innern mehrfach und zuletzt vor allem anläßlich meiner Prüfungen im Bundesamt für Verfassungsschutz und im Bundeskriminalamt 1981 meine Bedenken dargelegt. Bislang ist mir eine abschließende Stellungnahme des BMI zu diesem Fragenkreis aber noch nicht zugegangen.

Ebenfalls ist noch nicht abschließend zu meinen Bedenken gegen eine Übermittlung von bei Haus-

durchsuchungen oder bei Telefonüberwachungsmaßnahmen der Polizei gewonnenen Informationen an den Verfassungsschutz Stellung genommen.

Im Berichtsjahr wurde die Neuregelung der Amtshilfe des BGS für die Nachrichtendienste praktiziert. Dabei ist mit Erfolg das Verfahren einer stärkeren Spezifizierung angewandt worden, das es erlaubt, die einzelnen Verarbeitungsweisen restriktiver zu regeln, als bei Anwendung der Generalklauseln möglich wäre. Ich hatte in meinem letzten Tätigkeitsbericht angekündigt, daß ich die praktischen Auswirkungen der Neuregelung überprüfen und dann eine datenschutzrechtliche Wertung abgeben wollte. Da für eine Prüfung des Gesamtkomplexes Nachforschungen bei mehreren Stellen notwendig waren, habe ich bereits im Frühsommer mit Prüfungen bei verschiedenen Stellen des BGS begonnen. Prüfbesuche wurden bei den Grenzschutzstellen Lauenburg, Helmstedt und Hannover-Bahnhof sowie beim Grenzschutzamt Braunschweig durchgeführt. Seitens dieser Stellen wurde meine Prüftätigkeit in jeder Hinsicht unterstützt. Im August fand dann eine erste Prüfung beim BfV statt, die ohne Schwierigkeiten durchgeführt wurde. Aus technischen Gründen mußte der Abschluß der Prüfung auf November verschoben werden. Bei dem Versuch, im November die Prüfung zu beenden, kam es dann zu den an anderer Stelle (3.1.3) bereits geschilderten Schwierigkeiten. Meine Prüfung konnte erst im Dezember fortgesetzt werden, so daß hier eine Stellungnahme zur Neuregelung der Amtshilfe des BGS für die Nachrichtendienste aus datenschutzrechtlicher Sicht noch nicht möglich ist. Ich werde dies im nächsten Jahr nachholen.

Der Informationsaustausch zwischen Polizei und Nachrichtendiensten ist nach wie vor umfangreich. Schon dieser große Umfang des täglichen Auskunftsverkehrs macht es den Sachbearbeitern schwer, den Einzelfall sorgfältig zu prüfen. Den handelnden Beamten kann auch kaum vorgehalten werden, daß sie zuviel Übermittlungen zuließen, wenn gleichzeitig die Generalklauseln der innerdienstlichen Richtlinien weite Spielräume lassen und z. B. die Übermittlung an Verfassungsschutzbehörden generell zulassen (Nr. 3.5.4 der KpS-Richtlinien und Nr. 5.5.4 der Dateien-Richtlinien für das BKA; ebenso umfassend auch die Richtlinien über die Zusammenarbeit in Staatsschutzangelegenheiten).

Allerdings bessert sich dieses Bild in letzter Zeit. Bei den neuesten Errichtungsanordnungen für Dateien im BKA ist teilweise versucht worden, die Zulässigkeit der Übermittlung stärker einzugrenzen oder zu verdeutlichen als in den allgemeinen Dateien-Richtlinien. Bei der Formulierung bereichsspezifischer Verwaltungsvorschriften kommt es immer häufiger vor, daß einzelne Sicherheitsbehörden oder auch deren Abteilungen ihre jeweiligen fachspezifischen Belange (z. B. bei der Bestimmung der Speicherfrist) geltend machen. Dieser begrüßenswerte Schritt zu mehr Sachnähe hat aber notwendigerweise zur Folge, daß die Zweckbindung der Speicherung noch deutlicher betont werden muß. Wer z. B. aus den speziellen Anforderungen der Spionageabwehr heraus Daten länger speichern muß als sonst zulässig wäre, der darf diese Daten grundsätzlich auch nur für eben diesen Zweck verwenden.

Ein weiteres Problem bildet die Sicherstellung von Aktualität und Genauigkeit der zu übermittelnden Daten. Sicherheitsbehörden übermitteln sich nämlich gegenseitig in zahllosen Fällen Hinweise auf eingeleitete Verfahren oder Verdachtsmomente; bei den Empfängern werden diese Meldungen dann in der Regel gespeichert. Meist aber bleibt es bei dieser ersten Meldung; der Ausgang des Verfahrens, die Beseitigung des Verdachts oder auch dessen Erhärtung werden sehr oft nicht nachgemeldet. Dies wurde bei den Kontrollen durch meine Dienststelle in den vergangenen Jahren bei allen Sicherheitsbehörden immer wieder festgestellt. Wird über solche potentiell fehlerhaften Speicherungen Auskunft erteilt, so verstärkt sich die Gefahr, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. In verschiedenen von meinen Mitarbeitern überprüften Fällen wurden negative Angaben über Betroffene bei den Stellen gespeichert, die um diese Auskunft gebeten hatten, oder es erging sogar eine für den Betroffenen ungünstige Entscheidung. Da die verschiedenen Sicherheitsbehörden unterschiedliche Löschungsregelungen haben (Polizei: zehn Jahre, Nachrichtendienste: 15 Jahre als „Regelfrist", s. u. 3.2.3), kann es geschehen, daß eine Behörde, die über jemanden bei der Polizei nachfragt, dort zwar keine Auskunft erhält, weil die Akten inzwischen vernichtet sind, diese Auskunft jedoch noch von einem Nachrichtendienst bekommen könnte, der aufgrund einer ursprünglichen polizeilichen Meldung eine Akte über diese Person bei sich angelegt hat. Die Auskunft des Nachrichtendienstes wäre dann, wenn nicht in der Zwischenzeit noch Ergänzungen dort eingegangen sind, notwendig unvollständig, möglicherweise falsch.

Daraus folgt: Entweder darf bei so unklarer Situation keine Auskunft erteilt werden, oder es muß dafür gesorgt werden, daß die ursprünglichen Meldungen durch weitere Informationen über den Ausgang des betreffenden Verfahrens oder andere neuere Erkenntnisse ergänzt werden. Die speichernde Stelle muß jedenfalls in die Lage versetzt werden, die eigene Speicherung auf weitere Relevanz zu prüfen und, wenn sie die Informationen noch benötigt, zu aktualisieren. Diesem Anliegen dienen auch die Vorschriften Nr. 10 und 11 der Anordnung über Mitteilungen in Strafsachen (MiStra), wonach die Justizbehörden verpflichtet sind, der ursprünglich Anzeige erstattenden Behörde bzw. der Polizei den Ausgang des Verfahrens mitzuteilen. Diese Stellen sind ihrerseits verpflichtet, den neuen Sachverhalt, wie er sich aufgrund der Nachberichterstattung ergibt, an die Behörden weiterzugeben, die über die anfängliche Meldung unterrichtet worden waren. Leider geschieht dies im polizeilichen Bereich und auch bei den Nachrichtendiensten bisher nur selten. Es sind verschiedene Gespräche über dieses Thema geführt und Vereinbarungen getroffen worden, die eine Verbesserung der Praxis erwarten lassen.

Aber auch der andere Weg — Beschränkung der Übermittlung — sollte weiter beschritten werden. Grundsätzlich sollte keine Stelle Auskunft über Hinweise erteilen, die ihr nicht vollständig bekannt sind und die sie nicht selbst abschließend beurteilen kann. Von besonderen Ausnahmefällen abgesehen, in denen die Übermittlung auch ungesicherter Informationen verantwortet werden kann, sollte vor Erteilung der Auskunft nachgefragt werden, wie das Verfahren ausgegangen ist oder die Verdachtsmomente aufgeklärt worden sind, die früher einmal gemeldet worden waren. Im Bereich der Auskünfte, die das BKA als nationales Zentralbüro von Interpol erteilt, konnten nunmehr erste wichtige Schritte in dieser Richtung getan werden. Es wäre gut, wenn derartige Verfahrensregeln in den dienstlichen Vorschriften für die Sicherheitsbehörden generell festgeschrieben würden. Eine solche Verbesserung der Datenqualität würde auch der aktuellen Arbeit der Sicherheitsbehörden zugute kommen.

3.2.3 Überprüfungs- und Löschungsfristen, Behandlung der „Altfälle"

Daß personenbezogene Daten im Sicherheitsbereich grundsätzlich zu löschen sind, wenn sie nicht mehr für die Aufgabenerfüllung erforderlich oder geeignet sind, folgt aus den verschiedenen bereichsspezifischen Regelungen (z. B. § 100b Abs. 5 und § 163c Abs. 4 StPO, § 7 Abs. 4 G 10) und dem in allen Polizeigesetzen ausdrücklich verankerten verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit (vgl. z. B. § 2 Polizeigesetz NW). Dies ist prinzipiell auch unstreitig. Die Sicherheitsbehörden liefern in der letzten Zeit immer wieder Beweise dafür, daß sie die Lösungspflicht ernst nehmen.

Die in den letzten Jahren in Kraft getretenen Richtlinien über verschiedene Komplexe von Datenverarbeitung bei den Sicherheitsbehörden haben erkennbar dahin gewirkt, daß die Datenbestände reduziert werden. Freilich sind die Überprüfungsfristen teilweise noch nicht hinreichend differenziert. Für die Anfangszeit war es gewiß sachgerecht, die Überprüfung der weiteren Erforderlichkeit personenbezogener Daten im Polizeibereich nach zehn Jahren, bei den Nachrichtendiensten nach fünfzehn Jahren (als Regelfall) vorzuschreiben. Auf längere Sicht aber muß erörtert werden, ob die schutzwürdigen Belange der Betroffenen nicht zu einer weiteren Unterschreitung und Verkürzung bestimmter Fristen nötigen. Wenn und soweit Informationen auch über solche Tatbestände gespeichert werden dürfen, die noch nicht dasjenige Gewicht haben, das für die Einleitung eines Strafverfahrens vorausgesetzt wird — und dies ist bei den Nachrichtendiensten entsprechend ihrer Aufgabenstellung unverzichtbar, bei der Polizei in engen Grenzen hinnehmbar (siehe oben 3.2.1) —, dann müssen die Fristen zur Überprüfung und zur Lösung dieser Daten kürzer sein. Hierzu hat meine Dienststelle schon vor längerer Zeit Vorschläge unterbreitet. Es erscheint z. B. nicht vertretbar, für die Bereiche Staatsgefährdung und Landesverrat einerseits, „Extremismus" und Spionage andererseits gleiche Regelfristen festzulegen.

Die Bereitschaft zu solcher Differenzierung wächst bei allen Sicherheitsbehörden meines Zuständigkeitsbereichs. So sind bei der Polizei für einige Spezialdateien zwei- oder dreijährige Überprüfungsfristen festgelegt worden. Bei den Nachrichtendiensten werden ebenfalls verkürzte Überprüfungsfristen für bestimmte Bereiche eingeführt, zum Teil schon praktiziert.

Bei den verschiedenen Sicherheitsbehörden werden aber — in unterschiedlichem Umfang — noch zahlreiche Unterlagen aufbewahrt und bestehen entsprechende Speicherungen in den Dateien, die nach den heute geltenden Richtlinien nicht aufbewahrt bzw. gespeichert sein dürften, weil Aufbewahrungsfristen abgelaufen sind und keine neuen Erkenntnisse die weitere Speicherung rechtfertigen. Bereits vor Inkrafttreten des BDSG war nach der Rechtsprechung über die Aufbewahrung erkennungsdienstlicher und anderer sicherheitsbehördlicher Unterlagen nach Ablauf einiger Zeit im Einzelfall zu prüfen, ob die Unterlagen noch benötigt werden. Bei strikter Einhaltung dieser Rechtsprechung und des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit hätten bereits vor dem 1. 1. 1978 viele Daten gelöscht werden müssen. Durch das damals in Kraft getretene BDSG ist nochmals eine weitere Bereinigung der Dateien geboten worden. Die Verpflichtung zur umfassenden Bereinigung der Dateien bedeutet für die speichernden Behörden einen erheblichen Aufwand. Inzwischen sind bei den Sicherheitsbehörden meines Zuständigkeitsbereiches solche Bereinigungsaktionen im Gange (vgl. bereits 4. TB S. 22 f., 27, 30, 32 f.). Im BKA ist z. B. die Datei PIOS-Terrorismus um eine große Zahl von Datensätzen bereinigt worden. In der Abteilung Daktyloskopie des BKA sind über eine Million alter Unterlagen vernichtet worden. Im BfV waren, wie aus einer Erklärung des Amtes zu meinem Vierten Tätigkeitsbereich hervorgeht, bereits Ende des letzten Jahres rund eine halbe Million Notierungen gelöscht worden. Ich konnte diese Zahlen bislang nicht überprüfen, habe aber keinen Anlaß, ihre Richtigkeit zu bezweifeln.

Künftig werden nicht mehr benötigte Unterlagen voraussichtlich nicht mehr so lange aufbewahrt werden wie bisher. Denn nunmehr können in allen Dateien Fristen eingespeichert werden, bei deren Ablauf der entsprechende Vorgang „automatisch" herausgesucht und einem Sachbearbeiter zur Überprüfung auf weitere Notwendigkeit vorgelegt wird. Ich werde bei künftigen Prüfungen auch darauf achten, ob tatsächlich diese Fristen, wie vorgesehen, überall eingespeichert werden.

Vorläufig liegt jedoch noch ein bedeutendes Fehlerpotential darin, daß gespeicherte Daten, die bereits hätten gelöscht werden müssen, nach Fristablauf bei der Bearbeitung eines Vorgangs oder sonstwie aus dem Speicher abgerufen werden können. Sie dürfen dann grundsätzlich nicht verwertet, sondern müssen nunmehr unverzüglich gelöscht werden; die dazugehörigen Akten sind zu vernichten, und insbesondere hat eine Auskunft an andere Stellen zu unterbleiben. Ausnahmen hiervon scheinen mir nur in folgenden Fällen gerechtfertigt:

— Ergibt sich, daß bei fristgerechter Kontrolle die weitere Aufbewahrung und entsprechende Speicherung angeordnet worden wäre, so kann dies auch nachträglich verfügt werden.

— Ergibt sich, z. B. aus einer neuen Anfrage, die den Grund für die Wiedervorlage der alten Unterlagen bildet, daß nunmehr eine Bestätigung für die frühere Information vorliegt, so wird man jedenfalls bei bedeutsamen Fällen die weitere Aufbewahrung und Verwertung der Akte für vertretbar halten müssen, obwohl ursprünglich ein Verstoß gegen die Richtlinien vorlag.

Solche Fälle kommen u. U. bei der Spionageabwehr vor, wo relevante Informationen über lange Zeit hin Bedeutung haben können.

Dazu ein Beispiel: Eine Akte, die im Jahre 1960 wegen Verdachts nachrichtendienstlicher Tätigkeit zu Recht angelegt wurde, in der Zwischenzeit aber nie zur Bearbeitung gelangte (weil keine neuen Erkenntnisse oder Anfragen eingingen), wäre nach Inkrafttreten der neuen Frist gemäß den Dateien-Richtlinien im Jahre 1981 zu vernichten gewesen. Angenommen, die Vernichtung ist versehentlich unterblieben, und nunmehr fragt eine andere Sicherheitsbehörde im Jahre 1982 an, ob etwas über die Person vorliege, und teilt gleichzeitig mit, daß aufgrund bestimmter Anzeichen (aus neuerer Zeit) der Verdacht nachrichtendienstlicher Aktivität bestehe, so wird man nicht verlangen können, daß die Akte, die für die aktuellen Ermittlungen von Bedeutung sein kann, nunmehr allein deshalb vernichtet werden müsse, weil es bei Fristablauf nicht zu der vorgeschriebenen Prüfung gekommen war. Vielmehr ist in einem solchen Fall eine „Anreicherung" des neuen Verdachts durch die früheren Unterlagen vertretbar. Allerdings dürfen Daten, die eine frühere Verurteilung betreffen, im gerichtlichen Verfahren oder sonst im Rechtsverkehr nur im Rahmen von § 50 BZRG verwertet werden. Das Verwertungsverbot (§ 49 BZRG) steht aber nach wohl überwiegender Meinung in der Rechtslehre und auch nach Ansicht der Bundesminister der Justiz und des Innern einer Verwendung der alten Hinweise zur Aufklärung eines neuen Sachverhalts nicht entgegen — freilich nur solange es um eine interne Auswertung durch Polizei und Staatsanwaltschaft geht.

Durchbrechungen des Grundsatzes, daß Unterlagen, die hätten vernichtet werden müssen, nicht verwertet werden dürfen, müssen die Ausnahme bleiben. Selbstverständlich darf die gebotene Bereinigung der Bestände nicht deshalb „großzügiger" betrieben werden, weil man — ohne dafür Anhaltspunkte zu haben — auf später hinzukommende neue Erkenntnisse als nachträgliche Rechtfertigung spekuliert.

Um Mißverständnisse zu vermeiden, sei eines hinzugefügt: Der Datenschutz verlangt nicht, daß jede Akte nach Ablauf der betreffenden Frist sofort ungeprüft vernichtet wird. Die verschiedenen Richtlinien schreiben vielmehr eine Überprüfung auf weitere Erforderlichkeit vor. Wenn die eine oder andere Behörde aus arbeitsökonomischen oder sonstigen Gründen beschließt, bestimmte Gruppen von Altfällen unbesehen zu vernichten, so ist das nicht durch Gründe des Datenschutzes gefordert. Dies habe ich bei den Gesprächen mit den betreffenden Behörden deutlich gemacht.

3.2.4 Zum Auskunftsverhalten gegenüber dem Bürger

Das Unbehagen vieler Bürger an der Datenverarbeitung rührt zu einem wesentlichen Teil daher, daß sie nicht wissen, welche Daten in welchen Zusammenhängen über sie gesammelt und verbreitet werden. Mißtrauen und Vorbehalte gegenüber den Behörden lassen sich oft schon dadurch abbauen, daß den Betroffenen klare Auskunft über Art und Weise der Datenverarbeitung erteilt wird. Da dies bei Polizei und Nachrichtendiensten häufig nicht möglich ist, ohne die Aufgabenerfüllung ernstlich zu gefährden, hat der Gesetzgeber diese und einige weitere Behörden von der unbedingten Auskunftspflicht gegenüber den Betroffenen und der Veröffentlichungspflicht nach § 12 BDSG ausgenommen (s. auch § 19 Abs. 4 S. 4 bis 7 BDSG). Andererseits ist gerade in diesem Bereich das Bedürfnis der Bürger nach Informationen sehr groß; durch Offenheit kann gerade hier manches an Skepsis überwunden werden. Diese Einsicht ist in letzter Zeit auch bei den Verantwortlichen gewachsen. Die Polizeibehörden des Bundes haben schon seit längerer Zeit relativ großzügig Auskünfte an den Bürger erteilt — sei es unmittelbar, sei es mittelbar, indem ich ermächtigt wurde, dem Betroffenen das Prüfungsergebnis mitzuteilen. In den Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen und über die Führung von Dateien beim BKA ist mittlerweile ausdrücklich festgelegt, daß auf Antrag Auskunft darüber erteilt „wird", ob und ggf. welche Daten zur Person gespeichert sind, „es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen". Die Polizei muß daher zwischen den widerstreitenden Interessen abwägen und darf die Auskunft nur verweigern, wenn das Interesse an der Nichtherausgabe überwiegt. Zur Orientierung sagen die Richtlinien weiter, daß die Erteilung der Auskunft insbesondere in Betracht kommt, „wenn es sich um Unterlagen handelt, an deren Zustandekommen der Betroffene selbst beteiligt war und von denen er nach den Umständen annehmen kann, daß sie bei der Polizei aufbewahrt werden". Andererseits sind auch die Auskunftsverweigerungsgründe aus § 13 Abs. 2 Nr. 2 bis 4 BDSG in die Richtlinien aufgenommen worden, und als weiterer Verweigerungsgrund ist hinzugefügt, daß die Stelle, die die Daten angeliefert hat, die Auskunftserteilung ausgeschlossen hat. Errichtungsanordnungen für Dateien des BKA können eine generelle Regelung über die Auskunft enthalten.

Bundeskriminalamt, Bundesgrenzschutz und Bahnpolizei haben bisher in der weit überwiegenden Zahl der Fälle die beantragte Auskunft erteilt, sich also nicht auf die Ausnahmeklauseln berufen. Irgendwelche nachteilige Folgen für die Aufgabenerfüllung dieser Behörden sind dabei nicht bekannt-

geworden. Auch aus den Ländern, die nach meiner Kenntnis im großen und ganzen ebenso verfahren wie die Bundesbehörden, sind keine Störungen der polizeilichen Arbeit durch oder infolge von Auskünften an die Betroffenen bekanntgeworden. Selbstverständlich werden keine Auskünfte erteilt, durch die laufende Verfahren oder eine aktuelle polizeiliche Beobachtung beeinträchtigt würden, und bei schweren Straftaten wird auch in anderen Fällen nicht ohne weiteres Auskunft gegeben. Im übrigen besteht für die Polizei die Verpflichtung, im Rahmen anhängiger Strafverfahren Einvernehmen mit der Staatsanwaltschaft über die Auskunft herbeizuführen. Versuche, den genauen Erkenntnisstand der Polizeibehörden zu erforschen, dürften angesichts solcher Verfahrensweisen kaum erfolgversprechend sein.

Schwieriger ist es, das Auskunftsinteresse gegenüber den Nachrichtendiensten zur Geltung zu bringen. Aber auch hier ist zu differenzieren: Selbstverständlich wird niemand verlangen, Anfragen eines Spionageverdächtigen zu beantworten, und auch die Gefahr, daß noch unerkannte Agenten fremder Mächte sich durch eine „Negativauskunft" Sicherheit verschaffen wollen, ist nicht von der Hand zu weisen und kann deshalb Auskunftsverweigerungen rechtfertigen. Aber solche Erwägungen sind nicht unmodifiziert auf den Arbeitsbereich „Beobachtung extremistischer Bestrebungen" zu übertragen. Wenn schon die geheime Sammlung von Unterlagen über Bestrebungen im Sinne von § 3 Abs. 1 Nr. 1 Verfassungsschutzgesetz unvermeidlich ist, so kann doch das Interesse der Betroffenen, Denunziationen und Irrtümern entgegenzutreten und nicht durch unberichtigte Geheimdienstinformationen z. B. bei Bewerbungen für den öffentlichen Dienst beeinträchtigt zu werden, erhebliches Gewicht haben. Auch verfassungsrechtliche Überlegungen führen zu der Feststellung, daß dem Bürger das Auskunftsrecht gegenüber den Nachrichtendiensten nicht vollständig und für alle Fälle verweigert werden darf. Hierzu ist bereits auf die Rechtsprechung des BVerfG hinzuweisen, wonach der von Maßnahmen der Post- oder Telefonkontrolle Betroffene nachträglich benachrichtigt werden muß, „wenn eine Gefährdung des Schutzes der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes ausgeschlossen werden kann" (BVerfGE 30, 1, 21; dementsprechend § 5 Abs. 5 G 10 mit weiteren Verfahrensbestimmungen). Der vom BVerfG herangezogene verfassungsrechtliche Grundsatz der Verhältnismäßigkeit muß auch bei der Auslegung von § 13 Abs. 2 BDSG beachtet werden. Die Ansicht, daß auch die Verfassungsschutzbehörden unter bestimmten Voraussetzungen zu Auskünften und/oder Löschungen verpflichtet sind, setzt sich bei den Verwaltungsgerichten allmählich durch (vgl. VG Köln, Urteil vom 5. Mai 1982, Az. 14 K/8/81 und VG Berlin, Urteil vom 7. Juli 1982, Az. I A 9/81; beide Urteile sind noch nicht rechtskräftig).

Die Nachrichtendienste des Bundes geben bisher überwiegend keine Auskünfte über die gespeicherten Daten an die Betroffenen. Doch war es erfreulicherweise in den letzten Jahren zunehmend möglich, das BfV und den MAD in besonderen Einzelfällen davon zu überzeugen, daß zumindest eine Teilauskunft geboten und für die Aufgabenerfüllung des Dienstes unschädlich war. In einigen wenigen Fällen, in denen besondere Umstände vorlagen, fand sich auch der BND dazu bereit, mir eine detaillierte Auskunft an den Betroffenen zu ermöglichen. Durch solche Ansätze einer flexibleren Praxis konnten unnötige Ängste ausgeräumt werden.

Für die Zukunft stellt sich die Aufgabe, bestimmte Fallgruppen festzulegen, bei denen grundsätzlich eine Auskunft — sei es eine Teilauskunft, sei es die vollständige Information über alle vorliegenden Daten — vertretbar erscheint. Zu denken ist z. B. an die Sicherheitsüberprüfungen, die — wenn sie ordnungsgemäß im Rahmen der Richtlinien der Bundesregierung durchgeführt werden — den Betroffenen ohnehin bekannt sind. Die Überprüften wissen in diesen Fällen oder können wissen, daß Daten über sie beim BfV bzw. (für Personal, das dem Bereich des BMVg angehört) beim MAD oder (für eigene Mitarbeiter) beim BND vorhanden sind. Auch im Bereich „Extremismus" wird das Auskunftsproblem eher lösbar sein. Ich rechne nach den bisherigen Erfahrungen auf die Bereitschaft der Nachrichtendienste, sich auf die Erarbeitung entsprechender Richtlinien einzulassen.

Auf Unverständnis bin ich mit den Überlegungen zum Auskunftsrecht nur bei der Finanzverwaltung gestoßen. Der Bundesminister der Finanzen beharrt darauf, daß § 13 Abs. 2 BDSG es den Zollbehörden erlaube, ohne Begründung jegliche Auskunft zu verweigern. Die dargelegten verfassungsrechtlichen Grundsätze zum Auskunftsrecht werden vom BMF ebensowenig anerkannt, wie ihn bisher der Hinweis darauf überzeugt hat, daß so bedeutende Bundespolizeien wie der Bundesgrenzschutz, das Bundeskriminalamt und die Bahnpolizei dem Bürger mit einem erheblichen Maß an Offenheit gegenübertreten. Möglicherweise wird dieses Problem durch die geplante Novelle zum Bundesdatenschutzgesetz gelöst. Dort ist nämlich nach dem bisherigen Verfahrensstand vorgesehen, daß die geschilderte, bereits jetzt überwiegende Praxis für alle Polizeien gesetzlich verankert wird.

Es bleibt unbefriedigend, daß ich in den Fällen, in denen eine Behörde sich auf ihr Auskunftsverweigerungsrecht beruft, den Betroffenen nicht mitteilen kann, welches Ergebnis meine Prüfung hatte. Nicht ganz selten hielte ich eine Offenbarung an den Betroffenen für vertretbar, während die speichernde Sicherheitsbehörde aus grundsätzlichen Erwägungen bei der Geheimhaltung bleiben und damit den Betroffenen im unklaren lassen möchte, ob überhaupt etwas über ihn gespeichert ist oder war und wenn ja, was. Besonders problematisch ist es, daß deshalb auch nachträgliche Löschungen häufig nicht mitgeteilt werden können. Es sollte erwogen werden, ob nicht zumindest für besondere Ausnahmefälle eine Schlichtungsinstanz eingesetzt werden könnte, die — außerhalb der Regeln des Gerichtsverfahrens — über Auskunftsersuchen entscheiden könnte, die zwischen mir und der speichernden Stelle (in der Regel ein Nachrichtendienst) strittig sind.

3.2.5 Verfahren der Dateianfrage beim BfV

In meinem Vierten Tätigkeitsbericht (S. 29) habe ich darüber berichtet, daß ich bei datenschutzrechtlichen Kontrollen Praktiken im Rahmen der sog. Dateianfrage beim BfV feststellen mußte, die die Umgehung der einschlägigen Richtlinien zu Lasten der Betroffenen jedenfalls ermöglichten. So war es z. B. möglich, daß Bewerber für eine Stelle im öffentlichen Dienst ohne ihr Wissen und damit ohne die Chance der Rechtfertigung vom Verfassungsschutz überprüft wurden. Der BMI hat als Konsequenz aus meinen Feststellungen — so habe ich berichtet — alle obersten Bundesbehörden angeschrieben, eine genaue Einhaltung der Richtlinien über die Sicherheitsüberprüfung verlangt sowie einige weitere die zu Überprüfenden schützende Vorschriften erlassen. Ich habe angekündigt, daß ich die Einhaltung der Richtlinien in diesem Jahr erneut kontrollieren würde. Eine derartige Kontrolle kann sich nicht auf das BfV beschränken. Anhand der dortigen Unterlagen kann im wesentlichen nur festgestellt werden, welche Behörde wann über wen beim Verfassungsschutz nachgefragt hat. Ob die Anfrage zu Recht erfolgt ist, ob der Betreffende vorher informiert worden ist und ob die übermittelnden Daten zweckgerecht verwendet worden sind, kann nur bei der anfragenden Behörde geklärt werden.

Meine Versuche, dort Nachprüfungen anzustellen, mußte ich aber abbrechen, da sich mehrere Geheimschutzbeauftragte auf den Standpunkt stellten, ich hätte kein Recht, ihre Unterlagen einzusehen. Dies ist nach meiner Ansicht falsch, da mir nach § 19 Abs. 3 Satz 2 Nr. 1 BDSG ein Einsichtsrecht in alle Akten und Unterlagen zusteht, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Beim Verfahren der Dateianfrage geht es darum, daß mittels eines standardisierten Verfahrens personenbezogene Daten aus der Datei des Verfassungsschutzes übermittelt werden. Dieser Übermittlungsvorgang kann datenschutzrechtlich nur überprüft werden, wenn die Unterlagen bei der anfragenden Stelle eingesehen werden.

Ich habe deswegen den BMI mit Schreiben vom 6. September 1982 gebeten, gegenüber den Geheimschutzbeauftragten der obersten Bundesbehörden meine Prüfbefugnis klarzustellen und mir insbesondere eine entsprechende Nachprüfung beim BMI selbst zu ermöglichen. Bis zur Drucklegung dieses Berichts ist noch keine Antwort eingegangen. Sofern mir die Möglichkeit dazu gegeben wird, werde ich im kommenden Jahr das Verfahren der Dateianfrage datenschutzrechtlich überprüfen.

3.3 Bundeskriminalamt

3.3.1 Stand der Datenverarbeitung beim Bundeskriminalamt (Überblick)

Die Entwicklung der polizeilichen Datenverarbeitung hat beim Bundeskriminalamt — aber nicht nur dort — ein beachtliches Tempo angenommen. Welchen Ausbaustand inzwischen das polizeiliche Informationssystem erlangt hat und welche Realisierungsschritte demnächst anstehen, das machte die Tagung des Bundeskriminalamtes zum Thema „Polizeiliche Datenverarbeitung" im November 1982 in beeindruckender Weise deutlich. Es muß aber auch festgestellt werden, daß die Weiterentwicklung der elektronischen Datenverarbeitung bei der Polizei offenbar durch Datenschutzrücksichten kaum behindert wird. Die wesentlichen Kriterien der Fortentwicklung scheinen technische Reife, Erforderlichkeit im Sinne von Effizienzsteigerung sowie Kostengesichtspunkte zu sein. So war es jedenfalls den Ausführungen einiger hierzu referierender führender Polizeibeamter zu entnehmen. Dies verdient angesichts der manchmal zu hörenden Klagen, der Datenschutz behindere die polizeiliche Datenverarbeitung in unerträglichem Maße, festgehalten zu werden.

Versucht man die Entwicklung der polizeilichen Datenverarbeitung aus datenschutzrechtlicher Sicht zu kommentieren, so kommt es vor allem darauf an zu differenzieren. Zwar betreibt das Bundeskriminalamt seine Informationsverarbeitung in Zusammenarbeit mit den Ländern unter der Sammelbezeichnung INPOL, in Wirklichkeit handelt es sich hierbei aber um eine Zusammenfassung qualitativ höchst unterschiedlicher Anwendungen. Das INPOL-System besteht einerseits aus Teilen, bei denen es im wesentlichen um die Beschleunigung, Vereinfachung und mengenmäßige Bewältigung traditioneller kriminalpolizeilicher Arbeitsformen geht. Hier wird insbesondere die Überlegenheit des Computers an Schnelligkeit und an Kapazität zum Einsatz gebracht. Daneben kommen auch Verfahren zur Anwendung, die wesentliche qualitative Veränderungen gegenüber der bisherigen polizeilichen Tätigkeit mit sich bringen. Sie haben tiefgreifende datenschutzrechtliche Auswirkungen, aber auch Konsequenzen für die polizeiliche Sachbearbeitung. Im folgenden soll versucht werden, die wichtigsten Entwicklungslinien der Datenverarbeitung beim Bundeskriminalamt aufzuzeichnen und mit datenschutzrechtlichen Anmerkungen zu versehen.

3.3.2 Anwendungsbereiche von INPOL

Die wichtigsten Anwendungsbereiche des Gesamtsystems INPOL sind auf Bundesebene folgende:

a) Personen- und Sachfahndung

Die INPOL-Personen- und Sachfahndung hat das Fahndungsbuch herkömmlicher Art ersetzt. Mit ihrer Hilfe können Personen gesucht oder beobachtet werden bzw. als verloren oder gestohlen gemeldete Sachen wieder aufgefunden werden. Dieser Teil des INPOL-Gesamtsystems ist unumstritten. Hier hat die elektronische Datenverarbeitung Fortschritte für die polizeiliche Arbeit wie auch für den Datenschutz in nahezu gleicher Weise erbracht. Die Personen- und Sachfahndung ist auch dasjenige Programm, auf das die meisten Polizeibehörden Zugriff haben. Insgesamt sind es derzeit ca. 2 500 Terminals, von denen aus die Personen- und Sachfahndungsdaten abgerufen werden können.

b) Die Akten- und Personennachweissysteme

Mit Hilfe der Akten- und Personennachweissysteme kann die Polizei in sehr kurzer Zeit feststellen, ob eine Person „bekannt" ist bzw. ob eine Akte über sie existiert. Bislang wurde dieses System beim Bundeskriminalamt unter der Bezeichnung Zentraler Personenindex (ZPI) betrieben. An seine Stelle sollen in Zukunft der Kriminalaktennachweis (KAN), der Aktennachweis des Bundeskriminalamtes (BKAAN) und der Vorgangsnachweis Personen (VNP) treten. Im BKAAN sollen die „regionalen" (d. h. nur für das BKA bedeutsamen) Daten gespeichert werden, die nicht im überregionalen KAN erfaßt werden. Im VNP sollen lediglich reine Verwaltungsdaten erfaßt werden. Zu den damit zusammenhängenden Problemen wurde bereits im letzten Tätigkeitsbericht Stellung genommen.

Insbesondere durch die Einführung des KAN wird es im Aktennachweissystem der deutschen Polizei eine grundlegende Veränderung geben. Bislang war es im wesentlichen so, daß die Polizeibehörden in ihren Aktennachweissystemen ihre eigenen Akten verzeichnet hatten. Das Neue am KAN ist nun, daß überregional bedeutsame Akten auch überregional registriert und damit verfügbar werden. Dies bedeutet, daß beispielsweise eine Polizeibehörde in Hamburg einen Hinweis auf eine in München oder sonstwo existierende Kriminalakte erhalten kann. Will sie den Inhalt dieser Akte näher kennenlernen, so muß sie sich mit einem konventionellen Übermittlungsersuchen an die betreffende aktenführende Dienststelle wenden. Aus polizeilicher Sicht bedeutet dies eine erhebliche Verbesserung des Informationsflusses bei der Verbrechensbekämpfung, was bei der Diskussion über die regionale Abschichtung bisweilen übersehen wird. Wegen weiterer Einzelheiten der mit der Einführung des Kriminalaktennachweises verbundenen datenschutzrechtlichen Probleme verweise ich auf Abschnitt 3.3.5.

c) Die PIOS-Anwendungen

Auch die PIOS-Anwendungen erfüllen die Funktion eines Personen- und Aktennachweissystems. Darüber hinaus haben sie aber vor allem den Zweck, die Daten von Personen, Institutionen, Objekten und Sachen zu erfassen, zwischen ihnen Verknüpfungen herzustellen und systematische Auswertungen zu ermöglichen. Hier soll mehr erfaßt und ausgewertet werden als bloß der Name der „Hauptperson", gegen die sich ein Verfahren richtet, denn diese wäre auch bei einem herkömmlichen personenbezogenen Aktennachweissystem erfaßt. Die spezifische Arbeitsweise der PIOS-Dateien besteht darin, daß möglichst auch die Randpersonen, d. h. diejenigen, gegen die sich noch kein konkreter Verdacht richtet, erfaßt werden.

Das in einer Kriminalakte dokumentierte kriminalpolizeilich interessante oder zumindest relevant erscheinende Wissen soll „ausgewertet" werden. Durch Verknüpfung und Recherche im Wege der Verdachtsverdichtung sollen auch solche Personen als verdächtig ermittelt werden, die zunächst — bezogen auf die einzelne Information — noch nicht als verdächtig erscheinen.

Ein Wesensmerkmal der PIOS-Anwendungen ist deshalb die Erfassung der Personen, die nicht Verdächtige oder Beschuldigte sind, bei denen aber „zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies (die Speicherung) zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Straftaten, zur Ergreifung von zur Festnahme gesuchten Personen oder zur Abwehr einer im einzelnen Fall bestehenden erheblichen Gefahr erforderlich ist" (Ziffer 4.2.11 der Dateienrichtlinien, s. o. Nr. 3.2.1). In der Datei PIOS-Terrorismus sind dies vor allem die sogenannten „Kontaktpersonen", die im Rahmen der beobachtenden Fahndung, der Häftlingsüberwachung sowie der verdeckten Fahndung bekannt werden.

Eine Erfassung von „Randpersonen", deren Beteiligung an der Tat noch ungeklärt ist, betrifft notwendigerweise auch Personen, die — im nachhinein betrachtet — völlig unschuldig sind. Darüber hinaus besteht bei einem „Verdachtsverdichtungsinstrument" wie PIOS immer die Gefahr, daß quantitative Gesichtspunkte zu sehr in den Vordergrund treten. Wenn etwa ein Name zum dritten Mal auftaucht, liegt für viele der Schluß nahe, diese Person sei „auffällig".

Aus der Sicht des Datenschutzes kann den Gefahren, die mit den PIOS-Anwendungen verbunden sind, am ehesten durch ein differenziertes und kurz bemessenes Fristensystem und durch eine bessere Beachtung des Zweckbindungsprinzips begegnet werden. Gerade wenn die PIOS-Dateien insbesondere auch den „Noch-nicht-Verdächtigen" erfassen, dürfen über diesen Personenkreis nur in engen Grenzen Daten übermittelt werden. Sonst besteht die Gefahr, daß vage Verdachtsmomente weitergegeben werden, ohne daß der Betreffende die Chance einer Erklärung und Rechtfertigung erhält. Hier ist die Praxis aus meiner Prüfungserfahrung jedoch noch nicht als zufriedenstellend zu bezeichnen.

Ursprünglich wurde das PIOS-Verfahren zur Unterstützung der Bekämpfung der terroristischen Gewaltkriminalität entwickelt. Die Datei PIOS-Terrorismus habe ich im Jahre 1981 geprüft und die Ergebnisse im letzten Tätigkeitsbericht geschildert (vgl. dazu auch hier Nr. 3.3.8). Bereits im Jahre 1980 wurde die Datei PIOS-Rauschgift eingeführt. Im Jahre 1982 sind noch Errichtungsanordnungen für die „Arbeitsdatei PIOS-Landfriedensbruch und verwandte Straftaten" (APLF), die „Arbeitsdatei PIOS-Staatsgefährdung" (APSF), die „Arbeitsdatei PIOS-Landesverrat (APLV) und die „Arbeitsdatei PIOS-Waffen" (APW) bei mir eingegangen.

Dies zeigt, daß der weitere Ausbau der polizeilichen Datenverarbeitung mit großen Schritten vorangeht. Methoden, die zur Terrorismusbekämpfung entwikkelt worden sind, sollen nun auch Anwendung auf andere Arten von Kriminalität finden. Für die nächsten Jahre ist geplant, die Arbeitsdateien PIOS-Staatsgefährdung und PIOS-Terrorismus zu einer einheitlichen Datei „PIOS-Innere-Sicherheit" (APIS) zusammenzufassen.

Diese Entwicklung gibt aus datenschutzrechtlicher Sicht Grund zur Sorge. Was im Hinblick auf die Gefährlichkeit des Terrorismus und seine verdeckte, organisierte Arbeitsweise geschaffen und allgemein akzeptiert wurde, findet nun Anwendung auch in anderen Bereichen. Die Speicherung „anderer Personen" wird damit zu einer typischen Methode der computergestützten Verbrechensbekämpfung. Die damit zusammenhängenden datenschutzrechtlichen Probleme werden einen Teil der Aufmerksamkeit für die nächsten Jahre erfordern. Die Prüfung des Systems PIOS-Terrorismus und die nunmehr vom BKA zur Bereinigung unternommenen beträchtlichen Anstrengungen belegen, daß hier von Anfang an kurze Fristen festgelegt werden müssen, weil sonst Datenmengen entstehen, die kaum noch kontrollierbar sind. Die entsprechenden Errichtungs- und Feststellungsanordnungen sehen dies vor.

d) Straftaten/Straftäterdatei und Falldateien

Dateien besonderen Typs sind die Straftaten/Straftäterdatei und ihre Fortentwicklung, die Falldateien. Die Straftaten/Straftäterdatei wird nach einer bundesweiten Erprobung nunmehr ausschließlich vom Saarland bestückt. Eingegeben werden Angaben zu sämtlichen im Saarland angefallenen Delikten. Andere Bundesländer beliefern diese Datei nicht, können aber in Teilbereichen auf sie zugreifen. Da die Polizei des Saarlandes keine eigene Datenverarbeitungsanlage besitzt, erfolgt die Verarbeitung der Informationen beim BKA. Speichernde Stelle und somit mitverantwortlich für diese Datei ist auch das BKA.

Beim BKA unmittelbar werden Falldateien zu den Deliktbereichen Rauschgift (FDR) und Geiselnahme, Erpressung, Raub (FGER) betrieben.

Erreicht werden soll, daß bekannte Straftaten unbekannten Tätern zugeordnet werden können. Dies ist jedoch nur im Wiederholungsfalle oder bei weit verbreiteten Deliktsformen möglich. Die Erkenntnisse, die in diesem Zusammenhang gewonnen werden, sollen der Polizei Ermittlungsansätze für ihre Arbeit liefern. Inwieweit dies der Fall ist, kann derzeit noch nicht beurteilt werden. Es wird in Zukunft erörtert werden müssen, inwieweit die Erforderlichkeit für das Betreiben dieser Dateien gegeben ist. Ich habe sie bislang noch nicht überprüfen können. Ob sie besondere datenschutzrechtliche Probleme aufwerfen, kann nur nach einer gründlichen datenschutzrechtlichen Prüfung abschließend beurteilt werden. Ich beabsichtige eine derartige Prüfung durchzuführen.

e) Spurendokumentationssysteme (SPUDOK)

Dateien ganz neuen Typs sind die Spurendokumentationssysteme (SPUDOK's). Es handelt sich hierbei um eine Verfahrenshülle, die das Bundeskriminalamt für die Benutzung durch die Landeskriminalämter zur Verfügung stellt. Auch auf örtlicher Ebene können SPUDOK-Dateien betrieben werden. Der Zweck besteht darin, das Spurenaufkommen bei großen Ermittlungsverfahren zu dokumentieren, damit bei einer Vielzahl eingehender Hinweise und Spuren kein Informationsverlust eintritt.

Etwas vereinfacht könnte man sagen, daß SPUDOK an die Stelle des Notizblocks des ermittelnden Beamten getreten ist. Damit wird ebenfalls deutlich, welch tiefgreifende Veränderungen die polizeiliche Informationsverarbeitung im Zeitalter der Computer erfahren hat. Daß der Speicher eines automatischen Rechners unvergleichlich viel mehr faßt als ein Notizbuch, ist eine Binsenweisheit. Die sich daraus ergebenden Folgerungen sind es nicht.

Im Zeitalter der SPUDOK's braucht keine Information verlorenzugehen, kann auch die kleinste Spur verfolgt werden. Es muß aber auch keine Auswahl getroffen werden. Wo früher begrenzte Kapazität dazu zwang, mit kriminalistischem Spürsinn zwischen vermeintlich wichtigen und vermeintlich unwichtigen Spuren zu unterscheiden, kann im Rahmen von SPUDOK heute zunächst einmal alles gesammelt werden. Das erfaßbare Spurenaufkommen ist also wesentlich größer. Andererseits müssen all diese Spuren natürlich auch heute noch mit den herkömmlichen Mitteln der Kriminalistik „abgearbeitet" werden. Nach Abschluß des jeweiligen Ermittlungsverfahrens müssen alle Spuren endgültig ausgewertet und der Datenbestand gelöscht sein.

Datenschutzrechtlich wirft besonders die vielfältige Verwendbarkeit der SPUDOK's Probleme auf. Die Eigenschaft der SPUDOK's, nahezu alle erfaßten Textteile abgleichen zu können, eröffnet jedenfalls objektiv die Möglichkeit, mit Hilfe der Verfahrenshülle SPUDOK beliebige Sonderdateien einzurichten, die nicht unbedingt der Aufklärung großer Ermittlungskomplexe dienen müssen. So gesehen können die SPUDOK's sozusagen ein flexibles „Mehrzweckinstrument" sein.

Ein anderer Gesichtspunkt ist der, daß der Zugriff auf in einer SPUDOK gespeicherte Daten natürlich in anderer Weise geschieht als der auf ein polizeiliches Notizbuch — um noch einmal das Beispiel aufzugreifen. SPUDOK's können örtlich, überregional, landesweit, bundesweit oder aber in Kombination dieser Möglichkeiten betrieben werden. Mit der Eröffnung einer SPUDOK-Datei für einen weiteren Teilnehmer ist natürlich auch die Übermittlung der in der SPUDOK erfaßten Hinweise auf Verdächtige oder aus sonstigen Gründen Registrierte verbunden.

Ein weiteres Problem kann sich ergeben, wenn sich der Abschluß eines Verfahrens sehr lange verzögert. Umfangreiche Ermittlungsverfahren mit mehreren Tätern und Teilnehmern können unter Umständen solange als nicht aufgeklärt und abgeschlossen gelten, bis auch der letzte Täter überführt ist. Es ist durchaus denkbar, daß eine SPUDOK-Datei bei unaufgeklärten Verbrechen über Jahre hinaus aufbewahrt wird. Dagegen ist auch grundsätzlich nichts einzuwenden. Es muß aber betont werden, daß damit umfangreiche Datenbestände über Verdächtige und andere Personen aufgebaut werden. Aus datenschutzrechtlicher Sicht ist es von Bedeutung, daß diese Bestände dann nur zweckgebunden für das jeweilige Ermittlungsverfahren ver-

wendet werden, damit nicht unter der Hand Nebendateien entstehen, die auch für sonstige polizeiliche Zwecke, etwa für die Gefahrenabwehr, verwendet werden.

f) Digitales Sondernetz der Polizei

Bei dem digitalen Sondernetz der Polizei (Dispol) handelt es sich um ein im Aufbau befindliches Netz von Übertragungswegen und -systemen, das u. a. den Nachrichtenaustausch zwischen Polizeidienststellen mit unterschiedlichen Endgeräten (Datensichtstationen, Fernschreiber), aber auch den unmittelbaren Zugriff auf Informationssysteme anderer Behörden (z. B. BZR, KBA) technisch erleichtern soll. Mit Dispol wird der Informationsaustausch zwischen Polizei und anderen Behörden intensiviert, was aus meiner Sicht Auswirkungen auf den Datenschutz in diesem Bereich haben kann. Die Beurteilung von Dispol aus datenschutzrechtlicher Sicht wird ein Teil meiner künftigen Prüftätigkeit sein.

3.3.3 Die weitere Entwicklung

Die vorstehenden Ausführungen belegen, daß der Trend des Computereinsatzes bei der Polizei von der bloßen Unterstützung und Beschleunigung traditioneller Arbeitstechniken hin zu einem größeren Eigengewicht und Stellenwert der elektronischen Datenverarbeitung geht. Zu erwähnen wäre in diesem Zusammenhang auch die in diesem Jahr neue eingerichtete Datei TESCH, die der Auswertung extremistischen und terroristischen Schriftguts dienen soll. So gesehen ist es sicher nicht falsch zu behaupten, daß das eigentliche Computerzeitalter im Bereich der Polizeibehörden erst richtig beginnt. Allen gegenteiligen Appellen zum Trotz scheint „Kommissar Computer" erst am Beginn seiner Tätigkeit zu stehen. Unbehagen herrscht über diese Entwicklung nicht nur bei Datenschützern, sondern vielfach bei der Polizei selbst, wie dem aufmerksamen Zeitungsleser nicht entgangen sein wird. Der Parlamentarische Staatssekretär beim BMI, Spranger, hat bei der erwähnten Fachtagung des BKA ebenfalls auf diesen Gesichtspunkt hingewiesen.

Für die datenschutzrechtliche Diskussion dieser Entwicklung kommt es, wie im übrigen auch, darauf an, von pauschalen Schlagworten und Bewertungen wegzukommen. Es gibt nach meiner Auffassung keinen umfassenden Begriff, auf den unter datenschutzrechtlichen Gesichtspunkten die Entwicklung zu bringen wäre. Zu unterschiedlich sind die einzelnen neuen Dateien. Ich habe deswegen versucht, im Überblick aufzuzeigen, welches die jeweils spezifischen Wirkungen der neuen EDV-Aufwendungen sind und wie den mit den unbestreitbaren Fortschritten manchmal verbundenen neuen Gefahren am besten begegnet werden kann. Es wäre aber auch nicht richtig, die Probleme zu verharmlosen und zu übersehen, daß die Vielfalt der neu eingerichteten Dateien neue Probleme mit sich bringt. Eines davon besteht zum Beispiel darin, Löschungen durchgängig zu vollziehen und nicht eine Speicherung in einer Nebendatei zu „vergessen".

Wenn bisweilen zu hören ist, „der Datenschutz" stelle immer neue Forderungen, so geht es dabei in Wirklichkeit zumeist nur um eine Reaktion auf Weiterentwicklungen in der polizeilichen Datenverarbeitung. Ständig neue Dateien und Systeme erfordern ständig neue spezifische Anwendungsformen der datenschutzrechtlichen Grundgedanken. Das Tempo der Entwicklung wird weitgehend von der Technik und von der Frage bestimmt, in welchem Umfang neue Instrumente von der Polizei eingesetzt werden. Die Datenschutzbeauftragten können diese Entwicklung kaum beeinflussen, sie versuchen lediglich, mit ihr Schritt zu halten. Zur Resignation besteht aber kein Anlaß.

3.3.4 Anschluß des Bundeskriminalamtes an andere Informationssysteme

Die Polizei fordert nach wie vor einen Online-Anschluß an Informationssysteme der Ordnungsverwaltung und der Justiz, nämlich an die Dateien des Kraftfahrt-Bundesamtes, des Ausländerzentralregisters (AZR) und des Bundeszentralregisters. Der Anschluß an das AZR ist insofern bereits hergestellt, als das Bundeskriminalamt per Fernschreiber unmittelbar im dortigen System abfragen kann, ohne daß noch eine Entscheidung davorgeschaltet wäre.

Aus datenschutzrechtlicher Sicht bereitet das oben zu Nr. 2.7.2 bereits allgemein angesprochene Projekt ZEVIS, das im Aufbau befindliche zentrale Verkehrsinformationssystem, im hier zu erörternden Kontext am meisten Sorge, soweit es den Anschluß von Polizeibehörden an das System vorsieht.

3.3.5 Kriminalaktennachweis

Mit den Beschlüssen vom Juni 1981 zum zentralen Kriminalaktennachweis (KAN) beim BKA hat die Innenminister-Konferenz einen wegweisenden Schritt unternommen: Sie verzichtete nämlich auf Empfehlung der Datenschutzbeauftragten des Bundes und der Länder und unter Abkehr von früheren Modellen auf die vollständige zentrale Erfassung *aller* kriminalpolizeilich relevanten Unterlagen und beschränkte statt dessen den Aufbau des KAN auf Hinweise, die nach bestimmten pauschalierenden Kriterien überregionale Relevanz besitzen oder besonders schwere Straftaten betreffen. Hinweise auf lediglich regional bedeutsame Unterlagen sollen nur dezentral erfaßt werden.

Diese Abschichtung erfordert m. E. bereits der Wortlaut des BKA-Gesetzes. Sie ist aber jedenfalls ein Gebot des Grundsatzes der Verhältnismäßigkeit. Ausnahmen gelten — zu Recht — allein für die Fahndungs- und Haftdatei. Gefahndet wird stets überregional, und die Haftdatei muß zentral geführt werden, um unnötige Ausschreibungen zu vermeiden und falsche Identitätsangaben zu erkennen. Trotz der Abschichtung dürfte ein Großteil der Kriminalakten im überregionalen KAN registriert werden. Die Umschreibung dessen, was überregional bedeutsam ist oder besonders schwer wiegt, ist ent-

sprechend weit gefaßt. Als schwere und daher stets zentral zu registrierende Straftaten gelten demnach alle Verbrechen und alle in § 100a StPO aufgeführten Vergehen. Überregional bedeutsam sind Straftaten, „wenn der Verdacht besteht auf"

— gewohnheits-, gewerbs- oder bandenmäßige Begehung,

— Triebtäterschaft,

— planmäßige überörtliche Begehung,

— Handeln zur Verfolgung extremistischer Ziele,

— Begehung unter Mitführen von Schußwaffen,

— internationale Betätigung oder

— erneute Straffälligkeit der Beschuldigten oder Tatverdächtigen außerhalb ihres Wohn- oder Aufenthaltsbereichs.

Ich bin der Auffassung, daß mit diesen Formulierungen, die nicht alle Vorstellungen der Datenschutzbeauftragten berücksichtigen, die aber gemeinsam erarbeitet worden sind, alle Bedürfnisse für die überregionale Speicherung von Kriminalakten abgedeckt sind.

Allerdings laufen die Beschlüsse zum KAN weitgehend leer, wenn und weil nach Auffassung der IMK und des BMI die regionale Abschichtung nicht durchgängig gelten soll. Dies betrifft vor allem die Datei über erkennungsdienstliche Unterlagen (dazu unten Nr. 3.3.6).

3.3.6 Zentrale Registrierung erkennungsdienstlicher Unterlagen

Die vom Arbeitskreis II der IMK verabschiedeten und vom BMI für das BKA zum 1. Oktober 1982 in Kraft gesetzten „erkennungsdienstlichen Richtlinien" sehen (wie ihre Vorgänger) vor, daß alle erkennungsdienstlichen Unterlagen in einer Ausführung an das BKA übersandt und dort ausgewertet, verformelt und registriert werden. Die Registrierung erfolgt nicht nur nach den eigenen Merkmalen dieser Unterlagen (bei Fingerabdrücken: Formeln), sondern auch unter den Namen der Betroffenen. Ausgenommen von der Registrierung sind lediglich die Unterlagen, die nur zur aktuellen Identitätsfeststellung sowie zur Aufklärung von Ordnungswidrigkeiten angefertigt wurden (hier darf nur jeweils ein Vergleich mit den im BKA vorhandenen Unterlagen stattfinden, danach sind die übersandten Materialien zu vernichten). Dies ist eine Verbesserung, die neben verschiedenen anderen Fortschritten in der Neufassung der Richtlinien meinen seit 1979 vorgetragenen Anregungen Rechnung trägt.

Die zentrale Speicherung des Großteils der ed-Unterlagen im BKA hat jedoch folgende Konsequenz: Die Stellen, die auf den KAN zugreifen dürfen, erhalten neben dem Hinweis auf Fundstellen kriminalpolizeilicher Akten gleichzeitig Hinweise auf das Vorhandensein von ed-Unterlagen zu den betreffenden Personen. Wer aus Gründen der vorbeugenden Straftatenbekämpfung erkennungsdienstlich behandelt wurde, dessen Name wird auch dann im KAN verzeichnet, wenn die zugrundeliegende Straftat ihn nach den KAN-Kriterien *nicht* zu einem potentiell überregional tätigen Straftäter macht. Somit und insoweit läuft also die regionale Abgrenzung in den KAN-Richtlinien leer. Der KAN dient unter diesen Umständen nicht nur als Hilfsmittel zum Auffinden vorhandener ed-Unterlagen, sondern das Vorhandensein der ed-Unterlagen (auch aus nur regional bedeutsamen Zuammenhängen) bewirkt, daß gleichwohl eine Speicherung im überregionalen KAN stattfindet. Dadurch kann ein Verdacht gegen die betreffende Person begründet oder verstärkt werden, auch wenn die ed-Unterlagen selbst sie nicht als Tatverdächtigen ausweisen (sei es, weil am Tatort des aktuell aufzuklärenden Geschehens keine Spuren gefunden worden sind, sei es, weil die Vergleichsunterlagen nicht passen oder keinen sicheren Schluß ermöglichen).

Selbstverständlich müssen alle rechtmäßig erhobenen erkennungsdienstlichen Unterlagen möglichst vollständig ausgewertet werden, und es erscheint zweckmäßig, daß dies zentral geschieht. Dies wäre aber auch — und mit geringerer Belastung Unverdächtiger — möglich, wenn der Zugriff nur „anonym", über die ed-Unterlagen selbst und speziell über die verformelten Fingerabdrücke gestattet wäre. Die Auswertung gefundener Fingerabdrücke mit Mitteln der Daktyloskopie belastet die Personen, auf die diese hinweisen, nicht unangemessen; der hohe Grad an Zuverlässigkeit, den diese Methode gewährleistet, schließt Gefahren für Unbeteiligte durch Verwechslung und Fehlinterpretationen weitgehend aus, und wenn die Unterlagen keinen Schluß auf bereits bekannte Personen zulassen, dann kann aus ihnen auch kein Verdacht gegen irgendjemand hergeleitet werden.

Das Thema wäre nicht so bedeutsam, wenn man davon ausgehen könnte, daß ed-Unterlagen zu vorbeugenden Zwecken nur relativ selten angefertigt werden. Die Praxis zeigt aber, daß genau das Gegenteil der Fall ist. Dies mögen folgende Hinweise belegen:

— Der Bayerische Landesbeauftragte für den Datenschutz hat in seinem Tätigkeitsbericht für 1981 (Landtags-Drucksache 9/11712, S. 21 f.) im Zusammenhang mit den bekannten Vorfällen in Nürnberg im März 1981 festgestellt, daß damals die überwiegende Anzahl der in dem Jugendzentrum „KOMM" angetroffenen Jugendlichen erkennungsdienstlich behandelt wurde. Dies geschah, wie ich aus einer Eingabe in diesem Zusammenhang entnehmen konnte, sogar in Fällen, in denen die Identität bekannt war oder aber hätte festgestellt werden können. Eine Ausfertigung der Unterlagen wurde in jedem Fall an das BKA weitergeleitet. Dort wurden die Unterlagen in der ed-Datei gespeichert. Der BMI hat mir dazu mitgeteilt, daß er die Zuleitung von ed-Unterlagen auch in solchen Fällen für richtig halte, wobei die Entscheidung über die Erhebung der Unterlagen allein der zuständigen Polizeibehörde obliegt. Auch ich kann zur Zulässigkeit der Anfertigung der Unterlagen selbstverständlich nicht Stellung nehmen. Der Bayeri-

sche Landesbeauftragte hat aufgrund stichprobenartiger Prüfungen festgestellt, daß nicht nur in diesem Nürnberger Fall, sondern auch in anderen Fällen die Anfertigung von ed-Unterlagen ohne ausreichend strenge Prüfung der Voraussetzungen vorgenommen wird.

— Die Ausführungen des Bayerischen Landesbeauftragten dürften m. E. weitgehend auch für andere Bundesländer gelten. Dies belegen meine Erfahrungen aus den Prüfungen der Abteilung Staatsschutz des BKA in diesem Jahr und auch aus anderen Prüfungen, die ich seit 1979 durchgeführt habe. Bei den Meldungen für den Deliktsbereich Hausfriedensbruch mußte ich z. B. feststellen, daß fast in allen Fällen von den jeweiligen Landespolizeidienststellen ed-Unterlagen angefertigt wurden, und zwar offenbar weitgehend unabhängig davon, ob die Personen bereits bekannt waren oder nicht. Es ist davon auszugehen, daß diese ed-Unterlagen entsprechend den geltenden Richtlinien im allgemeinen auch in einer Ausfertigung an das BKA gegangen sind und dort gespeichert wurden.

— Einer Eingabe im Herbst dieses Jahres war zu entnehmen, daß in einem Fall von einer Landespolizeidienststelle ed-Unterlagen „wegen Bettelei und ähnlicher sonstiger Delikte" angefertigt und an das BKA übersandt wurden. Die Unterlagen wurden dort auch gespeichert, obwohl das BKA bereits aus der Angabe des Grundes hätte entnehmen müssen, daß die Unterlagen wohl kaum rechtmäßig angefertigt sein konnten. Der Fall ist inzwischen bereinigt, zeigt aber, wie schnell heute noch ed-Unterlagen angefertigt und im BKA gespeichert werden. Die gleiche Feststellung mußte ich verschiedenen anderen Eingaben in den letzten Jahren entnehmen.

Die Wirkungen der ohnehin zum Teil problematischen Praxis der Anfertigung von ed-Unterlagen wurden also durch die geltenden Richtlinien zur Übersendung von Ausfertigungen an das BKA und zur dortigen Speicherung noch verstärkt. Ich kann deshalb nur bedauern, daß der BMI und die Innenminister der Länder sich meinen Anregungen in diesem Punkt vollständig verschlossen haben, und hoffe, daß hier noch nicht das letzte Wort gesprochen ist.

3.3.7 Prüfung der Abteilung Staatsschutz des Bundeskriminalamtes

In der Zeit vom 7. September bis zum 7. Oktober 1982 habe ich bei der Abteilung Staatsschutz des Bundeskriminalamtes eine datenschutzrechtliche Prüfung durchführen lassen. Sie hat Gründe für Beanstandungen, aber auch Beispiele guter datenschutzrechtlicher Fortschritte erbracht. Beanstanden mußte ich eine Vielzahl von Speicherungen, die vor allem wegen Fristablaufs seit längerem zu löschen sind. In dieser Hinsicht hat die Prüfung ähnliche Ergebnisse wie die Prüfung bei anderen Sicherheitsbehörden erbracht. Die Abteilung Staatsschutz des Bundeskriminalamtes hat bislang ihre Daten im Verfassungsschutzcomputer NADIS gespeichert. In Zukunft wird BKA-St ein eigenes System hierfür in Form einer PIOS-Anwendung betreiben. Die Herauslösung der Bestände aus NADIS und ihre Überführung in PIOS bietet nach meiner Auffassung eine gute Gelegenheit, die bislang schon unternommenen Anstrengungen zur Bereinigung der Altfälle zu intensivieren und in einem absehbaren Zeitraum zum Abschluß zu bringen.

Bei den Speicherungen aus neuerer Zeit waren ebenfalls einige Fälle zu beanstanden. Insgesamt hat sich aber hinsichtlich der neueren Fälle ein positiver Gesamteindruck ergeben. Die KpS-Fristen sowie die Fristen aus den ergänzenden Richtlinien des BKA zu den KpS-Richtlinien führen im Ergebnis dazu, daß ein Großteil der bei BKA-St gespeicherten Fälle in Zukunft nach relativ kurzer Frist zur Wiedervorlage und damit in aller Regel zur Löschung kommt. Ein Bereinigungsproblem des Umfangs, wie es sich im Augenblick für das BKA hinsichtlich der älteren Vorgänge stellt, dürfte in Zukunft nicht mehr entstehen.

Grund für Beanstandungen gab eine Reihe von Fällen, in denen entgegen entsprechenden Richtlinien des BKA aus solchen alten Speicherungen Daten an andere Sicherheitsbehörden übermittelt worden sind. Beispielsweise wurde im Jahre 1979 über einen damals 66jährigen auf eine Anfrage im Rahmen einer Ordensverleihung die Information übermittelt, gegen den Betreffenden habe 1953 der Verdacht von Sprengstoffdiebstählen bestanden.

Auch Fälle der Datenübermittlung über Zeugen und Hinweisgeber, die nach den Dateienrichtlinien vom BKA in NADIS nicht mehr gespeichert sein dürften, mußte ich beanstanden.

Bedenken habe ich in einigen Fällen gegen die Praxis geäußert, Informationen über die zum Teil schon einige Zeit zurückliegende Einleitung eines Ermittlungsverfahrens zu übermitteln, ohne daß etwas über den Ausgang des Verfahrens bekannt ist. Nach meiner Auffassung wird in solchen Fällen ein Verdacht weitergegeben, der in der Zwischenzeit entweder bestätigt oder ausgeräumt hätte werden können.

Als Hauptproblem der Verarbeitung personenbezogener Daten bei der Abteilung Staatsschutz des Bundeskriminalamtes hat sich nämlich erneut die soeben erwähnte Tatsache herausgestellt, daß dort nur wenig über den Ausgang eingeleiteter Verfahren bekannt wird. In der Praxis sieht dies so aus, daß diejenige Polizeibehörde, die ein Ermittlungsverfahren einleitet, dem BKA nach den Richtlinien für den polizeilichen Meldedienst in Staatsschutzsachen hiervon Mitteilung macht. In aller Regel ist hiermit eine kriminaltaktische Anfrage verbunden; d. h. eine Anfrage, ob über die Person, gegen die das Ermittlungsverfahren eingeleitet wurde, beim BKA bereits etwas bekannt ist. An der Meldung über die Einleitung eines Verfahrens besteht also ein gewisses Eigeninteresse der Polizeidienststellen.

Es kann aus meiner Sicht nicht abschließend beurteilt werden, ob die das Verfahren einleitenden Polizeidienststellen von der Justiz über den weiteren

Fort- und Ausgang des Verfahrens unterrichtet werden. Das BKA jedenfalls erhält von den Polizeidienststellen bisher nur in seltenen Fällen Nachricht über den Fortgang des Verfahrens. Das Ergebnis ist, daß beim BKA zu einem hohen Prozentsatz nur die Einleitung eines Verfahrens, d. h. die Entstehung eines Verdachts bekannt wird, während der weitere Verlauf, d. h. die Bestätigung oder Verstärkung oder aber auch die Entkräftung des Verdachts nicht bekannt wird. Die justizielle Behandlung eingeleiteter Ermittlungsverfahren bleibt damit häufig ohne Einfluß auf die Speicherung beim BKA. Ziffer 5.4.3 der KpS-Richtlinien, wonach Unterlagen abweichend von den Regelfristen dann auszusondern sind, wenn die Ermittlungen oder eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichts ergeben, daß die Gründe, die zur Aufnahme in die KpS geführt haben, nicht zutreffen, läuft damit in vielen Fällen leer.

Ich habe das Problem mehrfach mit verantwortlichen Vertretern des BKA erörtert. Das BKA ist selbst sehr daran interessiert, über den Ausgang der Verfahren informiert zu werden. Wiederholte Apelle an die Länder haben bislang noch nicht den gewünschten Erfolg gebracht. Ich habe deswegen dem BKA auch im Anschluß an die Prüfung den Vorschlag unterbreitet, nach einer gewissen Frist von sich aus nachzufragen, ob sich ein bestimmter Verdacht bestätigt hat oder nicht. Ich hielte es für einen großen datenschutzrechtlichen Fortschritt, wenn das BKA zu einer derartigen Nachfrage, die nicht nur im Interesse des Betroffenen läge, bereit wäre. Im übrigen konnten das BKA und der BMI bislang zu meinem Prüfbericht, der erst im November fertiggestellt werden konnte, noch nicht Stellung nehmen.

3.3.8 Datei PIOS-Terrorismus

Im Jahre 1981 habe ich beim Bundeskriminalamt die Datei PIOS-Terrorismus geprüft und hierüber auch im Vierten Tätigkeitsbericht (S. 22) berichtet. Die Prüfergebnisse im einzelnen konnten im Tätigkeitsbericht nicht geschildert werden, waren aber Gegenstand mehrerer ausführlicher vertraulicher Beratungen im Innenausschuß des Deutschen Bundestages.

Der Bundesinnenminister hat inzwischen in mehreren Schreiben zu meinem Prüfbericht Stellung genommen. Insgesamt hatte ich in 25 Fällen bzw. Fallgruppen Speicherungen oder Verfahrensabläufe beanstandet. Der Bundesminister des Innern hat in allen Fällen die Beanstandung als berechtigt anerkannt, zu einem Fall hat er jedoch mitgeteilt, daß die Prüfung noch nicht endgültig abgeschlossen sei. Die von mir kritisierten Speicherungen sind entweder bereits gelöscht — so die große Mehrzahl — oder es wird an ihrer Bereinigung und Löschung gearbeitet. Da eine einzelne Beanstandung nicht selten hunderte oder gar tausende von Speicherungen betreffen kann, ist es nicht verwunderlich, daß die Bereinigungsarbeit ihre Zeit dauert.

Im Bundeskriminalamt hat am 4. Januar 1982 eine 13köpfige Arbeitsgruppe „Aktenbereinigung TE“ die Arbeit aufgenommen. Sie hat in nunmehr einjähriger, bisweilen mühevoller Kleinarbeit die systematische Bereinigung von PIOS begonnen und bereits bis zu einem bemerkenswerten Stadium vorangetrieben. Der Zeitpunkt, an dem alle PIOS-Speicherungen in vollem Einklang mit den Vorschriften, insbesondere den Dateien-Richtlinien stehen, ist demnach absehbar.

Im einzelnen wurden seit der Erstellung meines Prüfberichts ca. 25 000 Personendatensätze gelöscht, was ca. 20 % der Bestände in PIOS-TE ausmacht. Zusammen mit den bereits vor meiner Prüfung vorgenommenen Bereinigungen ergibt sich daraus eine beträchtliche Verringerung der Zahl der gespeicherten Datensätzen. Der weitere Fortgang der Bereinigungsarbeiten wird in dieser Hinsicht noch weitergehende Veränderungen erbringen.

Seit dem 1. Januar 1982 wird bei Neueinspeicherungen in PIOS auch ein Wiedervorlagedatum mit eingegeben. In einer Sonderaktion wird das Wiedervorlagedatum rückwirkend für die seit 1. März 1981 erfolgten Neueinspeicherungen nachgetragen. Dadurch wird es in Zukunft möglich sein, die unterschiedlichen Fristregelungen der Dateien-Richtlinien einzuhalten.

Für die Dauer der Bereinigungsarbeiten schreiben die ergänzenden Regelungen des Bundeskriminalamtes zu den KpS-Richtlinien vor, daß aus Vorgängen keine Datenübermittlung mehr vorgenommen werden darf, wenn sie wegen Fristablaufs oder aus anderen Gründen zur Löschung anstehen, aus Gründen der Arbeitskapazität aber noch nicht gelöscht werden konnten.

Zum Bereich der Häftlingsüberwachung hat der Bundesminister des Innern für das Bundeskriminalamt mit Wirkung zum 1. Oktober 1982 eine vorläufige Teilregelung erlassen. Einzelheiten dieser Neuregelung können hier nicht erörtert werden. In ihrer Gesamttendenz trägt die Neuregelung meinen Bedenken gegenüber der früheren Regelung und meinen im Anschluß an die PIOS-Prüfung gemachten Vorschlägen im wesentlichen Rechnung. Eine pauschale Speicherung aller Häftlingskontakte wird es demnach in Zukunft nicht mehr geben. Relevanzprüfung und abgestufte Fristenregelung dürften dafür sorgen, daß in Zukunft im Bereich der Häftlingsüberwachung keine Speicherung von personenbezogenen Daten im bisherigen Umfang mehr stattfindet.

Insgesamt läßt sich aus der Prüfung des Systems PIOS und aus den nachfolgenden Diskussionen der Schluß ziehen, daß vergröbernde Verallgemeinerungen den datenschutzrechtlichen Problemen nicht gerecht werden. Das Bundeskriminalamt jedenfalls war unbeirrt von der im Anschluß an den letzten Tätigkeitsbericht in der Öffentlichkeit bisweilen heftig geführten Diskussion bereit, die Konsequenzen aus der in meinem Prüfbericht enthaltenen Kritik zu ziehen. Das Ergebnis sind nicht nur aus datenschutzrechtlicher Sicht erfreuliche Fortschritte für die Betroffenen, sondern auch die Vernichtung inzwischen irrelevant gewordener Daten-

bestände, die der Effizienz der Arbeit sicher nicht immer dienlich waren.

3.3.9 Interpol

a) Die Grenzen sind zumindest in Westeuropa für jedermann durchlässig geworden. Dieses Umstandes bedienen sich gesetzestreue Bürger ebenso wie Straftäter. Nicht nur deswegen, sondern auch aus vielen anderen Gründen haben Straftaten heute nicht selten internationale Bezüge. Die Polizei versucht dem durch internationale Zusammenarbeit gerecht zu werden. Zur gegenseitigen Unterstützung ist die internationale kriminalpolizeiliche Organisation (Interpol) gegründet worden. Jedes Mitgliedsland hat ein Nationales Zentralbüro errichtet. In der Bundesrepublik Deutschland ist dies das BKA. Ihm wurde diese Aufgabe durch § 1 Abs. 2 BKAG zugewiesen.

Die Zusammenarbeit besteht vor allem im Nachrichtenaustausch der Nationalen Zentralbüros, der weitgehend durch das Generalsekretariat in Paris vermittelt und organisiert wird. Letzteres hat nach den Statuten u. a. den Auftrag, als internationale Informationszentrale zu dienen, ähnlich wie dies innerstaatlich Aufgabe des BKA ist.

Im Zusammenhang mit der Aufgabe als internationales Informationszentrum der Kriminalpolizei werden vom Generalsekretariat vor allem folgende Informationsersuchen durchgeführt:

— Internationale Ausschreibungen zur Festnahme zwecks Auslieferung,

— Ermittlung des Aufenthalts von Straftätern und Zeugen,

— Ersuchen um Identifizierung hilfloser Personen oder von Straftätern,

— Ersuchen um Überwachen vermuteter international agierender Straftäter.

Zur Erfüllung seiner Aufgaben unterhält das Generalsekretariat eine manuell betriebene zentrale Namenskartei. Diese umfaßte zum 1. Januar 1980 über 2 Mio. Registrierungen. Daneben bestehen mehr als 100 Spezialkarteien, die ebenfalls manuell betrieben werden.

Eine Automatisierung der Zentralkartei ist geplant. Auf diese automatisierte Datei sollte nach Vorstellung von Interpol künftig auch jedes Nationale Zentralbüro zugreifen können. Die Realisierung dieses Projekts (Arbeitstitel: Fichier Informatisé des Recherches) dürfte sowohl aus finanziellen als auch aus datenschutzrechtlichen Gründen (hierzu s. u.) auf absehbare Zeit nicht möglich sein.

Für die Beziehungen zwischen dem BKA als Nationalem Zentralbüro und anderen Nationalen Zentralbüros sowie dem Generalsekretariat von Interpol gelten die allgemeinen und besonderen innerstaatlichen Rechtsvorschriften, gegebenenfalls in Verbindung mit Verpflichtungen aus völkerrechtlichen Verträgen. Für das BKA sind § 11 S. 3 BDSG und das BKAG in Verbindung mit den Dateienrichtlinien, den Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen oder Sonderregelungen wie § 28 Abs. 4 der 1. Waffenverordnung einschlägig.

Das Generalsekretariat von Interpol stützt sich für seine Tätigkeit bisher allein auf die Statuten. Ihnen kommt jedoch keine völkerrechtliche Verbindlichkeit zu, weil sie nicht in verbindlicher Form vereinbart sind. Im Jahre 1982 ist ein Sitzstaatsabkommen mit Frankreich abgeschlossen worden.

b) Die „möglichst umfassende gegenseitige Unterstützung aller Kriminalpolizeien“ im Rahmen von Interpol soll, so heißt es in Artikel 2 der Statuten, „im Geiste der Erklärung der Menschenrechte“ erfolgen. Eine der Methoden des Schutzes der Menschenrechte ist der verantwortungsvolle Umgang mit personenbezogenen Informationen. Datenschutzrechtliche Regelungen der Interpolarbeit haben also in den Interpol-Statuten einen unmittelbaren Anknüpfungspunkt.

Über die Notwendigkeit konkreter Datenschutzregelungen besteht seit längerem Einvernehmen mit dem BKA und dem Generalsekretariat der Interpol-Organisation. Von meiner Dienststelle wurden dem BKA erstmals 1979 Vorschläge unterbreitet, insbesondere:

— Es sollen klare und rechtsverbindliche (d. h. auf völkerrechtlichem Wege zustandegekommene) Regeln für die datenverarbeitende Tätigkeit des Generalsekretariats von Interpol und das Verhältnis zu den Nationalen Zentralbüros erarbeitet werden, die Kriterien für die Sammlung, Auswertung, Speicherung, Übermittlung und Löschung von Daten enthalten;

— Es muß gewährleistet sein, daß Auflagen etc., die das BKA an die Auskunft knüpft (z. B. Beschränkung auf bestimmte Verwendungszwecke, Fristen zur Vermeidung der Umgehung des Verwertungsverbots von § 49 BZRG), eingehalten werden.

— Es ist eine unabhängige und externe Kontrolle für die Dateien beim Generalsekretariat zu schaffen, deren Entscheidungen das Generalsekretariat binden;

— Der Bürger muß ein Recht auf Auskunft (gegebenenfalls durch Vermittlung des externen Kontrollorgans) erhalten, soweit nicht der Zweck der polizeilichen Tätigkeit gefährdet ist.

Das BKA hat meine Vorschläge weitgehend übernommen und in die Beratungen der Interpol-Gremien eingebracht. Die Mehrheit der Mitglieder ist ihnen jedoch in verschiedenen Punkten nicht gefolgt.

Am 11. Oktober 1982 hat die Generalversammlung von Interpol auf ihrer 51. Sitzung eine Ergänzung der Statuten beschlosssen, die eine Lösung der datenschutzrechtlichen Probleme bewirken soll. Diese Beschlüsse enthalten eine

Reihe von Regelungen über die informationellen Beziehungen der Nationalen Zentralbüros zum Generalsekretariat sowie über die informationelle Tätigkeit des Generalsekretariats selbst und dessen Kontrolle. Bei strikter Beachtung dieser Regelung können beachtliche Verbesserungen gegenüber der bisherigen Situation erreicht werden. Allerdings leidet die von Interpol beschlossene Regelung an drei Mängeln:

— Die Regelungen enthalten bisher keine klaren Löschungskriterien.

  Zwar gilt seit 1979 für die Interpol-Zentrale eine interne Löschungsregelung; sie sieht für die Speicherung der Daten von Personen über 65 oder 70 Jahren, die international ausgeschrieben waren, nach Ablauf von zehn Jahren die Löschung vor, wenn inzwischen keine weitere Dotierung erfolgte. Bei anderen Personen soll eine Löschung nach der gleichen Zeit erfolgen, wenn der Registrierung Hinweise zugrunde liegen, die keine internationale Relevanz besitzen und somit für die Interpol-Zentrale im Grunde gar nicht speicherwürdig waren. Im übrigen erfolgt aber nach dieser Regelung (mit Ausnahme von Daten über Verstorbene) keine Löschung bzw. Vernichtung von Personenspeicherung und -akten. Das betrifft vor allem den sicher umfangreichen Personenkreis, über den im Wege der Auswertung des Nachrichtenaustausches Hinweise vorliegen, die als international relevant erachtet werden. Diese Regelung ist insgesamt noch unbefriedigend.

— Schwerer wiegt jedoch, daß die Regelung keine eindeutig externe und unabhängige Kontrolle vorsieht. Die Tätigkeit des Kontrollorgans wird vielmehr stets als „interne Kontrolle" bezeichnet. Es ist auch nicht vorgesehen, daß der Betroffene den Rechtsweg gegen das Generalsekretariat von Interpol beschreiten kann. Die bindende Wirkung der Entscheidung des Kontrollorgans ist ebenfalls nicht eindeutig geregelt.

— Außerdem enthält die Regelung keinerlei Hinweise über ein Auskunftsrecht des Betroffenen. Auch das interne Kontrollorgan wird nach der Regelung nur ermächtigt, dem Betroffenen mitzuteilen, daß die Prüfung vorgenommen wird.

Eine Unterkommission der internationalen Konferenz der Datenschutzbeauftragten hat im März 1982 auf der Grundlage von Vorschlägen eines Thesenpapiers, das ich im Auftrag der Konferenz vorgelegt hatte, Beschlüsse gefaßt, die im wesentlichen mit meinen Vorschlägen gegenüber dem BKA (s. o.) übereinstimmen.

Auf der Vierten Internationalen Konferenz der Datenschutzbeauftragten im Oktober 1982 in London wurden die Beschlüsse der Interpol-Generalversammlung im Grundsatz begrüßt. Aus den vorstehend angeführten Gründen wurde jedoch betont, daß der wirkliche Wert der Datenschutzregelungen für Interpol erst nach einiger Zeit aufgrund praktischer Erfahrungen ermessen werden könne. Die erwähnte Unterkommission wird sich deshalb weiter mit den datenschutzrechtlichen Fragen im Zusammenhang mit der Tätigkeit von Interpol und der Realisierung der neuen Regelung befassen müssen.

c) Eine in diesem Jahr von mir durchgeführte Prüfung des Informationsaustauschs zwischen Interpol und BKA hat eine Reihe von Punkten aufgezeigt, bei denen bei Zugrundelegung der Maßstäbe des § 11 BDSG Anlaß zu erheblichen datenschutzrechtlichen Bedenken bestand.

— Es wurden Auskünfte an ausländische Stellen erteilt, ohne daß ein ausreichender Anfragegrund angegeben war oder ohne daß überhaupt eine Anfrage vorlag. So widersprachen sich in einem Fall die Anfragegründe, ohne daß dies bemerkt wurde; in einem anderen Fall ging der Anfragegrund erst nach Erteilung der Auskunft ein; in einem dritten Fall war zu einer Person ein Hinweis aus dem Ausland erteilt worden, ohne daß um Auskunft ersucht worden war; seitens des BKA wurde dennoch über diese Person im Inland eine Rundumfrage abgehalten. Der größte Teil der Hinweise wurde dann — ohne Zusammenhang mit der Meldung — an das ausländische Zentralbüro übermittelt.

  In anderen Fällen wurde die Auskunft nicht auf den jeweils konkret bezeichneten Anfragegrund beschränkt.

  Beispiele: In einem Fall (Anfrage auf dem Hintergrund eines Terrorismusverdachts) wurden Hinweise an das Ausland wegen angeblicher Störung einer mündlichen Verhandlung beim Bundesgerichtshof übermittelt, obwohl dies weder relevant war noch sich aus den Akten überhaupt die Richtigkeit dieser Auskunft ergab. In einem anderen Fall wurden ebenfalls auf Anfrage wegen Terrorismusverdachts u. a. Hinweise über einen vermuteten Diebstahl und über das Privatleben übermittelt, die von einer Landespolizeibehörde an das BKA berichtet wurden.

— Oft erfolgten Hinweise auf Ermittlungsverfahren, die zum Teil fünf oder noch mehrere Jahre zurücklagen und deren Verfahrensausgang nicht bekannt war (zur innerstaatlichen Problematik dieses Verfahrens s. oben 3.2.2). Soweit dann später der Ausgang des Verfahrens aus irgendeinem Grunde dennoch bekannt wurde, erfolgte keine entsprechende Nachmeldung an die ausländische Behörde.

  Die jeweiligen Beispiele ließen sich vervielfachen. Ich habe gegenüber dem BKA deutlich gemacht, daß hier alles unternommen werden muß, um derartige relativ häufige Pannen zu vermeiden. Das BKA hat in seiner Antwort auf meinen Bericht zu erkennen gegeben, daß es bereit ist, meinen Anregungen künftig weitgehend Rechnung zu tragen. Einige meiner Vorschläge wurden jedoch abgelehnt, weil dies einen zu großen Arbeitsauf-

wand bedeute (insbesondere die Nachprüfung der weiteren Relevanz ursprünglich gespeicherter Daten vor der Übermittlung an andere Nationale Zentralbüros; nur Hinweise auf staatsanwaltschaftliche Ermittlungsverfahren sollen nachgeprüft werden). Ich halte es aber für wichtig, daß gerade im Informationsaustausch mit dem Ausland besondere Sorgfalt angewandt wird; ist eine Nachricht erst einmal aus dem Einflußbereich deutscher Behörden herausgelangt, so ist es schwierig, die Belange der Betroffenen zu wahren.

3.3.10 Erfassung von Zigeunernamen im INPOL-System

Verschiedene Veröffentlichungen im Verlaufe des vergangenen Jahres geben Anlaß, zur Speicherung sogenannter „Zigeunernamen" in INPOL besonders Stellung zu nehmen. In der Personendatei des Informationssystems der Polizei werden im Datenfeld PSN (sonstiger Name) unter anderem Künstlernamen, Ordensnamen, Geschiedenennamen und frühere Namen von Personen eingestellt, die in der Personenfahndungsdatei ausgeschrieben sind. Erfaßt wird auch der Zigeunername, wenn eine ausgeschriebene Person dieser Volksgruppe angehört. In einer Eingabe hatte sich der Verband Deutscher Sinti e. V. gegen diesen nach seiner Meinung diskriminierenden Zusatz in INPOL gewandt. Ich habe aufgrund dieser Eingabe die Angelegenheit mit dem Bundeskriminalamt und dem Bundesministerium des Innern ausführlich erörtert. In einer ersten Stellungnahme hatte das Bundeskriminalamt gegenüber dem Bundesministerium des Innern erklärt, daß nach seiner Auffassung die Kennung eines sonstigen Namens im Datenfeld PSN als Zigeunername aus kriminalpolizeilicher Sicht nicht erforderlich sei, da es nicht erheblich sei, wie man die sonstige Personalie bezeichne, denn nur der konkrete Name selbst ist Suchbegriff in INPOL. Das Bundesministerium des Innern hat aufgrund dieser Stellungnahme das BKA im Jahre 1981 gebeten, den Begriff „Zigeunername" nicht mehr zu verwenden und den entsprechenden Namen als „sonstigen Namen" ohne weitere Zusätze zu speichern. Das BKA sollte sich dafür einsetzen, daß auch die Polizeidienststellen der Länder von der Verwendung des Begriffs „Zigeunername" absehen. Wie ich nunmehr erfahren mußte, hat jedoch der Arbeitskreis II der Innenminister-Konferenz im Juni 1982 beschlossen, den Begriff „Zigeunername" doch weiter zu verwenden. Eine ursprünglich erfreuliche Änderung einer Speicherungspraxis wurde somit zurückgenommen (siehe auch Drucksache 9/2360).

3.4 Bundesgrenzschutz

Bei der Grenzschutzdirektion (GSD) in Koblenz wird eine Personendatei für den Bundesgrenzschutz geführt, auf die nur die Grenzschutzdirektion Zugriff hat. Die Anlieferung von Informationen der Grenzschutzstellen erfolgt auf konventionellem Wege. Diese Datei des Bundesgrenzschutzes dient dem Nachweis über die bei der Grenzschutzdirektion und hier insbesondere bei der Zentralstelle für die Bekämpfung der unerlaubten Einreise von Ausländern vorhandenen Erkenntnisse. Der bisher mögliche Zugriff des Bundeskriminalamtes auf diesen geschützten Teil des zentralen Personenindex ist inzwischen ausgeschlossen.

Innerhalb des INPOL-Fahndungsbestandes erfaßt die Grenzschutzdirektion in einem geschützten Bestand, auf den neben der Grenzschutzdirektion nur die Grenzdienststellen des Bundes Zugriff haben, solche Personen, die von der GSD (als Zentralstelle zur Bekämpfung der unerlaubten Einreise von Ausländern) zur Fahndung, Aufenthaltsermittlung, polizeilichen Beobachtung ausgeschrieben sind, sowie solche Personen, die von der Grenzschutzdirektion im Auftrag anderer Dienststellen nach Maßgabe der Zusammenarbeitsrichtlinien ausgeschrieben worden sind. Der in meinem Vierten Tätigkeitsbericht als bedenklich geschilderte Zugriff der Staatsschutzdienststellen des Bundeskriminalamtes und der Landeskriminalämter ist nunmehr nicht mehr möglich.

In meinem Vierten Tätigkeitsbericht habe ich außerdem eine Prüfung der vorstehend erwähnten geschützten Personendatei des Bundesgrenzschutzes angekündigt. Wegen umfangreicher anderer Prüfungen, insbesondere beim Bundeskriminalamt und beim Militärischen Abschirmdienst (siehe Nr. 3.3.7, 3.3.8, 3.6 dieses Berichts), war es mir nicht möglich, diese Prüfung durchzuführen, ich habe sie aber in den Prüfungsplan für das kommende Jahr aufgenommen.

3.5 Bundesamt für Verfassungsschutz

Das nachrichtendienstliche Informationssystem NADIS dient in erster Linie der Registrierung bestimmter Personengrunddaten und dazugehöriger Aktenzeichen. Eingabe- und abfrageberechtigt sind das BfV und die Landesämter für Verfassungsschutz. Die Abteilung Staatsschutz des Bundeskriminalamtes hat bisher ebenfalls Datensätze in NADIS eingespeichert und insoweit auch Zugriff. Neben der NADIS-Personenzentraldatei (PZD) werden beim BfV noch Sonderdateien geführt, die ich bislang nur zum Teil prüfen konnte. Diese Sonderdateien enthalten eine über die Registrierfunktion hinausgehende erweiterte Speicherung von Informationen, die prinzipiell nur den damit befaßten Stellen zugänglich sind.

Im letzten Tätigkeitsbericht (S. 28) hatte ich die Frage angeschnitten, in welchem Umfang Daten über einzelne Personen beim Bundesamt für Verfassungsschutz gespeichert werden dürfen, insbesondere ob auch einfache Mitglieder beobachteter Organisationen oder nur deren „Träger", d. h. im wesentlichen die Funktionsträger erfaßt werden können. Nach meiner Ansicht ist letzteres der Fall, weil das BfV primär nicht zur Registrierung von Personen, sondern zur Beobachtung verfassungsfeindlicher Bestrebungen zuständig ist. Die Speicherung der Daten über Personen muß nach meiner Überzeugung — von Spezialbereichen wie Spiona-

geabwehr oder Sicherheitsüberprüfung einmal abgesehen — für die Beobachtung entsprechender Organisationen erforderlich oder zumindest diesem Primärzweck untergeordnet sein (so auch im Grundsatz VGH Bad.-Württ., Urteil v. 14. 9. 82, DÖV 1982, 1041, 1042). Andernfalls besteht die Gefahr, daß aus der Beobachtung von Organisationen mehr und mehr die Beobachtung einzelner Personen wird. Letzteres kann, insbesondere soweit es die aktive Wahrnehmung von Grundrechten wie der Meinungs- und Demonstrationsfreiheit betrifft, nachteilige Auswirkungen auf eben jene Grundrechte haben. Es macht selbstverständlich schon rein quantitativ einen erheblichen Unterschied, ob das BfV lediglich die Träger beobachteter Organisationen speichert oder auch Mitglieder und Teilnehmer an bestimmten Aktionen.

Ich habe in meinem letzten Tätigkeitsbericht ausdrücklich darauf hingewiesen, daß es hier Meinungsunterschiede mit dem BfV gibt und das Amt auch eine andere Praxis übt. Wenngleich diese Praxis mit der Auffassung der Bundesregierung im Einklang steht (vgl. Bundestags-Drucksache 9/1889 v. 30. Juli 1982), halte ich auch weiterhin eine Diskussion dieses Fragenkreises für notwendig. Möglicherweise kann am Ende dieser Diskussion eine differenzierte Sichtweise stehen, die sowohl nach den in Betracht kommenden Organisationen unterscheidet als auch andere, dem Verhältnismäßigkeitsprinzip gerecht werdende Unterscheidungsmerkmale berücksichtigt. Ich denke hier an eine verstärkte Anwendung der Zeitspeicherung und an eine bessere Durchsetzung des Zweckbindungsprinzips. Wenn Verdachtsfälle zu dem Zweck der weiteren Aufklärung gespeichert werden, so sollten sie nach meiner Ansicht auch nur für diesen Zweck verwendet werden. Ich werde die Gespräche mit dem BfV zu diesem Fragenkomplex fortsetzen.

Ebenfalls noch nicht endgültig geklärt sind die Fragen, die ich im vergangenen Jahr unter dem Stichwort „Zusammenarbeit von Verfassungsschutz und Polizei" (4.TB S. 29) aufgeworfen habe. Über die allgemeine Amtshilfeproblematik und das speziell im Verhältnis Polizei/Nachrichtendienste geltende, verfassungskräftige Trennungsgebot hinaus hatte ich besonders das Problem angeschnitten, ob es mit §§ 108, 110 StPO vereinbar ist, wenn die Polizei bei Hausdurchsuchungen gewonnene Daten an den Verfassungsschutz übermittelt. Wortlaut und Sinn der §§ 108, 110 StPO stehen nach meiner Ansicht einer undifferenzierten Datenübermittlung in diesen Fällen entgegen. Weder kann es angehen, daß die Polizei routinemäßig die bei Hausdurchsuchungen gewonnenen Daten, etwa Karteien, Adreßverzeichnisse etc. an den Verfassungsschutz übermittelt, noch halte ich es für zulässig, daß diejenigen Daten, die die Polizei für das von ihr betriebene Ermittlungsverfahren nicht braucht, an den Verfassungsschutz übermittelt werden. Eine Hausdurchsuchung stellt einen schweren Eingriff in die Privatsphäre dar, der nur für bestimmte Zwecke und bei Einhaltung relativ eng gefaßter Verfahrensvorschriften zulässig ist. Wenn es zum Zweck des Verfahrens, in dessen Rahmen die Hausdurchsuchung durchgeführt wird, notwendig ist, beim Verfassungsschutz Rückfrage zu halten, so hält sich auch die im Rahmen einer derartigen Anfrage notwendige Datenübermittlung noch im Rahmen der Zweckbindung. Wenn also beispielsweise beschlagnahmtes Adreßmaterial nicht zugeordnet werden kann, so bewegt sich eine Nachfrage beim Verfassungsschutz im Rahmen des anhängigen Strafverfahrens. Die oben beschriebene „routinemäßige" Übermittlung von bei Hausdurchsuchungen gewonnenen Daten dient aber nicht mehr dem Zweck des Strafverfahrens und läßt den Verfassungsschutz mittelbar an einem polizeilichen Instrument, eben der Hausdurchsuchung, teilhaben, das ihm selbst von Gesetzes wegen nicht zusteht.

Die Telefonüberwachung durch die Nachrichtendienste ist im Gesetz zu Artikel 10 des Grundgesetzes geregelt. Dort sind auch die Voraussetzungen und insbesondere die Kontrollinstanzen („Abhörkommission") für Abhörmaßnahmen der Nachrichtendienste festgelegt. Die Strafprozeßordnung eröffnet der Polizei unter den in §§ 100a und 100b beschriebenen Voraussetzungen die Möglichkeit, den Fernmeldeverkehr zu überwachen. Die in § 100b StPO festgelegten Verwertungsvorschriften stehen nach meiner Ansicht einer Übermittlung der bei dieser Überwachung gewonnenen Daten — es sei denn, wie oben bei der Hausdurchsuchung, zum Zweck der Nachfrage im Rahmen des konkreten Strafverfahrens — entgegen. Eine andere Praxis würde darüber hinaus möglicherweise auch geeignet sein, die Bestimmungen des Gesetzes zu Artikel 10 GG objektiv zu unterlaufen. Der BMI hat im Rahmen der Beratung meines Vierten Tätigkeitsberichts im Innenausschuß des Bundestages ausgeführt, er wolle das Problem in Abstimmung mit dem Bundesjustizminister klären. Für die Zeit dieses Abstimmungsprozesses würden beim BfV keine Informationen mehr aus Verfahren der Polizei nach § 100a StPO gespeichert. Ich begrüße dies und hoffe, daß eine Entscheidung in absehbarer Zeit getroffen werden kann. Sollte sie im Einklang mit meiner Auffassung stehen, so halte ich es für geboten, auch aus früheren Jahren stammende Informationen, die die Polizei durch Maßnahmen nach § 100a StPO gewonnen und an das BfV übermittelt hatte, aus den Akten zu tilgen. Bei meinen Prüfungen stoße ich — so auch in diesem Jahr — gelegentlich auf derartige Unterlagen.

Zum Problem der „Altfälle" wurde wenige Tage nach Erscheinen meines letzten Tätigkeitsberichts bekanntgegeben, daß vom BfV inzwischen 500 000 Notierungen in NADIS gelöscht worden sind. Diese Zahl belegt, welche Anstrengungen das BfV zur Bereinigung inzwischen unternommen hat, und zeigt andererseits, daß meine Kritik nicht ganz unberechtigt war. Ich werde auch in meiner weiteren Prüftätigkeit darauf achten, daß die Bestände des BfV kontinuierlich weiter bereinigt werden.

Zu der von mir im Jahre 1981 geprüften Sonderdatei beim BfV, über die auch im Vierten Tätigkeitsbericht (S. 28) berichtet wurde, ist mir bislang noch keine abschließende inhaltliche Stellungnahme zugegangen. Der BMI hat mir mitgeteilt, daß er eine Arbeitsgruppe eingesetzt hat, die die gesamte Datei

einer umfassenden Prüfung unterzogen hat. Im Zusammenhang mit der Prüfung dieser Sonderdatei hatte ich auch einige Beanstandungen zu Einzelfällen ausgesprochen. Einigen dieser Beanstandungen hat der BMI bereits Rechnung getragen, zu den übrigen soll eine Entscheidung nach Abschluß der Prüfung des Gesamtkomplexes getroffen werden. Bis zur Fertigstellung dieses Berichts war die Gesamtprüfung noch nicht abgeschlossen.

Im Jahre 1982 wurden im Bereich des Bundesamtes für Verfassungsschutz nur Einzelfälle nachgeprüft. Bei der Bearbeitung von Bürgereingaben konnten weitere Fortschritte erzielt werden. In einigen Fällen wurde die Löschung, in anderen eine kurze Überprüfungsfrist vereinbart. Erfreulicherweise ist die Zahl derjenigen Fälle gestiegen, in denen vollständig oder doch wenigstens teilweise Auskunft erteilt werden konnte. Hier bahnt sich vielleicht eine Tendenz zu verstärkter Transparenz an. Ich halte dies für eine notwendige Konsequenz aus einigen — allerdings nicht rechtskräftigen — verwaltungsgerichtlichen Urteilen aus jüngster Zeit, in denen festgestellt worden ist, daß auch der Verfassungsschutz bei der Entscheidung über ein Auskunftsersuchen nach dem BDSG eine Ermessensentscheidung im Einzelfall treffen muß (s. oben Nr. 3.2.4). In der weiteren Konsequenz dieser Rechtsprechung sehe ich es als wichtig an, daß stärker zwischen den einzelnen Fachbereichen der Verfassungsschutzarbeit unterschieden wird. Ein Auskunftsersuchen, das sich auf einen Spionagefall bezieht, ist anders zu behandeln als ein Auskunftsersuchen aus dem Extremismusbereich. Wenn das BfV mir mitteilt, daß Daten über einen Petenten nicht gelöscht werden könnten, weil zwar seit Jahren keine neuen Erkenntnisse mehr über ihn angefallen seien und die extremistische Organisation, der er angehörte, nicht mehr existiere, über ihn aber „keinerlei entlastende Erkenntnisse etwa in Richtung einer Abkehr vom Extremismus ..." vorlägen, so frage ich mich, wie ein Bürger sich rechtfertigen und entlastende Erkenntnisse dem Verfassungsschutz mitteilen soll, wenn er von einer Speicherung und deren Grund gar nichts weiß.

Ich habe mich gegen Versuche gewandt, Daten von Personen beim Verfassungsschutz allein deswegen zu speichern bzw. unter den Verfassungsschutzbehörden auszutauschen, weil sie sich mit Eingaben an die Behörde oder eine Aufsichtsinstanz gewandt hatten. Hier bleibt es bei der im BfV bislang schon geübten Praxis, wonach eine Eingabe nicht zur Speicherung führt und auch ansonsten keinerlei Nachteil für den Petenten hat.

Insgesamt war die Prüfungstätigkeit beim BfV bis zum Sommer des Berichtsjahres von keinen Störungen beeinträchtigt. Leider hat sich dieses Bild inzwischen geändert. Nachdem ich im Sommer 1982 eine Nachprüfung des Komplexes „Amtshilfe des BGS für die Nachrichtendienste" beim BfV begonnen hatte, wollte ich die Prüfung Mitte November zum Abschluß bringen. Dies war aber nicht möglich, weil das BfV seine Auffassung zum Umfang meiner Prüfkompetenz geändert hatte und dementsprechend eine Prüfung in der bisherigen Art nicht mehr durchführen ließ. Die Einzelheiten hierzu sind an anderer Stelle (Nr. 3.1.3) beschrieben. Fürs erste konnte ich meine Prüfbefugnis inzwischen wieder in vollem Umfang wahrnehmen. Ich hoffe, daß dies auch in Zukunft möglich sein wird.

3.6 Militärischer Abschirmdienst

Im vergangenen Jahr habe ich eine umfangreiche, mehrmonatige datenschutzrechtliche Prüfung beim Amt für Sicherheit der Bundeswehr, der Zentrale des Militärischen Abschirmdienstes, durchführen lassen. Die bereits im Jahr zuvor bei den MAD-Gruppen in Kiel, Düsseldorf und München erfolgten Prüfungen wurden dadurch ergänzt und zum Abschluß gebracht. Die Prüfung erstreckte sich auf die wichtigsten Dateien des MAD sowie die dazugehörigen Akten und Materialien. Wegen der außerordentlichen zeitlichen Dauer der Prüfung verdient es besonders festgehalten zu werden, daß die verantwortlichen Mitarbeiter des MAD die Prüfung in jeder Phase unterstützt haben und ein Maß an Kooperation gezeigt haben, das es erlaubte, sich von vornherein auf die wichtigsten inhaltlichen Fragen zu konzentrieren.

Die Prüfung hat eine Reihe von datenschutzrechtlichen Mängeln ergeben, die ich beanstanden mußte. Gründe der Geheimhaltung lassen lediglich eine allgemein gehaltene Schilderung der festgestellten datenschutzrechtlichen Verstöße zu.

— Beim MAD gibt es so wie bei fast allen Sicherheitsbehörden das Problem der „Altfälle", d. h. von Fällen, die wegen Fristablaufs oder wegen geänderter Zuständigkeit zu löschen sind. Auf dieses Problem habe ich bereits in meinem letzten Tätigkeitsbericht (S. 32) hingewiesen. Beim MAD kommt erschwerend hinzu, daß in früheren Jahren eine genaue Abgrenzung zur Zuständigkeit des Verfassungsschutzes praktisch fehlte. Im Ergebnis führte dies zur Speicherung von Daten über eine Vielzahl von Personen, die allenfalls extremistisch, aber nicht „zersetzend" tätig waren. Für die Extremismusbeobachtung ist der Verfassungsschutz zuständig. Dem MAD obliegt lediglich die „Zersetzungsabwehr", d. h. die Abwehr von extremistischen Angriffen gegen die Bundeswehr.

— Bereits vor meiner Prüfung hat es beim MAD Bestrebungen gegeben, den eigenen Zuständigkeitsbereich in dem oben beschriebenen Sinn enger zu fassen. Mit Hilfe einer neuen Zentralen Weisung sollen die spezifischen Aufgaben des MAD präziser umschrieben werden. Für die Zukunft kann demnach davon ausgegangen werden, daß die Tätigkeit des MAD sich neben anderen — unbestrittenen — Bereichen auf die reine Zersetzungsabwehr konzentriert. Dies bedeutet aber gleichzeitig das Erfordernis der Löschung einer Vielzahl von Speicherungen, die aufgrund des früheren, weiteren Aufgabenverständnisses zustande gekommen sind.

— Auch beim MAD war wie schon zuvor bei anderen Sicherheitsbehörden festzustellen, daß aus derartigen „Altvorgängen" auf Anfrage noch Da-

ten übermittelt wurden. Die Beeinträchtigung der schutzwürdigen Belange der Betroffenen vervielfacht sich dadurch, daß zu der rechtswidrigen Speicherung die Übermittlung der Daten an eine andere Sicherheitsbehörde hinzutritt, was bei jener eine neue Speicherung zur Folge haben kann.

— Anlaß zur Beanstandung gaben auch einzelne gespeicherte Daten. Es handelte sich dabei um Informationen, die in Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts als dem innersten Kern des Persönlichkeitsrechts zugehörig bezeichnet werden können.

— Große Bedenken habe ich auch gegen die zum Teil gebräuchliche Praxis geäußert, Informationen mit teilweise belastendem Inhalt ohne Aktenrückhalt in der Datei zu speichern. Nach meiner Ansicht muß die Nachvollziehbarkeit und damit eventuell auch Beweisbarkeit von gespeicherten Daten gewährleistet sein.

Neben den Beanstandungen habe ich auch eine Reihe von Empfehlungen und Verbesserungsvorschläge ausgearbeitet und unterbreitet. Sie beziehen sich vor allem auf die Organisation der nunmehr anstehenden Bereinigungsarbeiten und auf das Auskunftsverhalten bis zum Abschluß der Bereinigung. Außerdem habe ich Vorschläge für differenzierte Zugriffsregelungen, für den künftigen Umfang der in den Dateien zu speichernden Daten sowie für eine stärkere Beachtung des Zweckbindungsprinzips gemacht. Für den Bereich der Zersetzungsabwehr habe ich ergänzende Abgrenzungsvorschläge unterbreitet. Auch wenn die reine Extremismusbeobachtung in Zukunft wohl dem Verfassungsschutz überlassen bleibt, ergeben sich noch eine Fülle von Abgrenzungsfragen mit unmittelbar datenschutzrechtlichem Bezug. Insbesondere bei Werbung für Kriegsdienstverweigerung und bei verschiedenen Aktivitäten der Friedensbewegung stellt sich manchmal die Frage, was „schon" zersetzend ist. Ich habe zu diesem Problemkreis Vorschläge gemacht, mit deren Hilfe nach meiner Auffassung die zulässige Zersetzungsabwehr von unzulässiger Einwirkung auf Grundrechte abgegrenzt werden kann.

Sowohl der MAD als auch der Bundesminister der Verteidigung haben inzwischen erste Stellungnahmen zu meinem Prüfbericht abgegeben. Die Beanstandungen wurden bis auf zwei Fälle, in denen noch klärende Gespräche geführt werden müssen, als berechtigt anerkannt. Die Löschung beanstandeter Speicherungen sowie die Umstellung beanstandeter Verfahren wurden zugesagt. Die von mir gemachten Empfehlungen wurden als überwiegend vom Ansatz her berechtigt oder sachgerecht angesehen, eine endgültige Stellungnahme zu den meisten von ihnen steht noch aus.

Damit hat sich eine Entwicklung fortgesetzt, die sich bereits bei den Prüfungen der MAD-Gruppen in Kiel, Düsseldorf und München angedeutet hatte. Der MAD steht dem Bundesdatenschutzgesetz und den sich daraus ergebenden Konsequenzen für die eigene Arbeit aufgeschlossen gegenüber. Die datenschutzrechtlichen Kontrollen werden akzeptiert und unterstützt, auch wenn sie zu Beanstandungen führen. Bereits vor meinen Prüfbesuchen hatte der MAD mit einer umfassenden Neuformulierung seiner Richtlinien begonnen, um damit die Konsequenzen aus dem Erlaß des BDSG zu ziehen. So war es nicht verwunderlich, daß ich mit meinen Beanstandungen und Empfehlungen teilweise auf „offene Türen" stieß. Für die Zukunft leite ich daraus die Hoffnung ab, daß die Bereinigung der mit dem Datenschutzrecht nicht in Einklang stehenden Speicherungen zügig betrieben wird und daß bei den Neueinspeicherungen die neuen Richtlinien beachtet werden.

3.7 Bundesnachrichtendienst

3.7.1 Art der verarbeiteten Daten

Der BND befaßt sich mit Aufgaben der Auslandsaufklärung, der Gegenspionage und Spionageabwehr. Hauptziel hierbei ist die Gewinnung von Sachinformationen (vgl. auch § 3 G 10). Die Sachdaten werden zu Berichten an die politischen Führungsgremien aufbereitet. Insoweit stellen sich keine Fragen des Datenschutzes.

Das auf die Gewinnung von Sachinformationen gerichtete Hauptinteresse bedingt aber auch die Speicherung von personenbezogenen Daten. Das gilt z. B. für Mitarbeiter des BND, für die der BND auch die Sicherheitsüberprüfungen durchführt. Außerdem ist der BND u. a. mit der Beobachtung des internationalen Kommunismus sowie anderer internationaler Aktivitäten befaßt, die für die politischen Entscheidungsgremien von Bedeutung sind. In all diesen Bereichen, die hier nicht abschließend aufgeführt oder näher erläutert werden können, erfolgt auch personenbezogene Datenverarbeitung. Sie betrifft in beachtlichem Umfang auch inländische Bürger, soweit Zusammenhänge mit den Aufgaben des BND bestehen.

3.7.2 Form der Verarbeitung

Die personenbezogene Speicherung von Daten erfolgt u. a. in automatisiert geführten Dateien. Die Dateien haben im wesentlichen die Funktion von Fundstellennachweisen. Die Zugriffsberechtigung ist intern abgestuft und eingeschränkt, so daß nur ganz wenige Stellen eine umfassende Auskunfts- und Zugriffsberechtigung auf die Dateien haben. Dies gebietet schon das Eigeninteresse des BND.

Der Umfang des zu registrierenden Personenkreises und die Voraussetzungen der Löschung sind durch interne Bestimmungen geregelt. So sind Datensätze, die 15 Jahre lang nicht mehr ergänzt wurden, auf weitere Erforderlichkeit zu überprüfen. Durch Einspeicherung des Erfassungsdatums ist seit 1976 gesichert, daß die Akte fristgemäß vorgelegt wird. Fälle, die vor dieser Zeit registriert wurden, müssen gesondert auf weitere Speicherwürdigkeit geprüft werden.

Neben den automatisiert geführten Dateien bestehen in bestimmten Arbeitsbereichen manuell ge-

führte Karteien. Aufgrund meiner Prüfungen wurden nunmehr in weitgehender Übereinstimmung mit Anregungen meiner Dienststelle adäquate einheitliche Regelungen erlassen, die für die externe wie interne Kontrolle unentbehrlich sind. Allerdings wird — ebenfalls auf meine Anregung hin — noch überprüft, ob die Führung von Karteien in diesen Dienststellen überhaupt erforderlich ist. Auskünfte erfolgen konventionell im Wege der Einzelanfrage oder durch Bandabgleich. Daß die Auskunftserteilung zur Vermeidung von Fehlern zentralisiert ist, dürfte sich für den Datenschutz günstig auswirken.

3.7.3 Informationen von anderen Behörden

Der Gesetzgeber hat dem BND (wie anderen Sicherheitsbehörden auch) gegenüber verschiedenen Behörden unter bestimmten Voraussetzungen *Auskunftsansprüche* eingeräumt (z. B. Bundeszentralregister, § 39 BZRG, Meldebehörden, § 18 Abs. 3 MRRG, Sozialleistungsträger, § 72 SGB X).

Daneben partizipiert der BND jedoch — ähnlich wie das BfV und auch andere Sicherheitsbehörden — an den Informationen oder der Datenverarbeitung anderer Stellen. Dies geschieht nach Maßgabe innerdienstlicher Regelungen oder Vereinbarungen. Nach meinen Prüfungsergebnissen erfolgt dies zum einen in der Form, daß technische Verbindungen bestehen, die einem Online-Anschluß zu der Datei einer anderen Behörde gleichkommen. Hier bestehen Probleme, die einer Lösung bedürfen; ich bin darüber mit den zuständigen Stellen im Gespräch.

Die zweite Möglichkeit besteht darin, daß im Rahmen eines speziell geregelten und bestimmten Verwaltungsaufgaben dienenden Verfahrens die Möglichkeit geschaffen wird, daß der BND mit den vom Verfahren betroffenen Personen Verbindung aufnehmen kann, um diese nach Erkenntnissen zu befragen, die für seinen Auftrag notwendig sind. Aufgrund meiner Anregungen ist bei der zweiten Fallgruppe dafür gesorgt, daß die Personen vor der Befragung von den Vertretern des BND auf die Freiwilligkeit ihrer Angaben hingewiesen werden sowie darauf, daß die Bereitschaft zu Aussagen gegenüber dem BND keinen Einfluß auf das Verfahren selbst hat. Außerdem wurde zugesagt, anderen Behörden über diese Angaben und Personen nur unter ganz engen Voraussetzungen Auskunft zu erteilen. Insoweit bestehen daher aus datenschutzrechtlicher Sicht keine Bedenken mehr.

Der dritte Bereich der Partizipation ergibt sich jetzt aus der Neuregelung der Amtshilfe zwischen BGS und den Nachrichtendiensten. Hiernach unterrichtet der BGS den BND entweder auf besonderen Antrag oder aus eigener Initiative über bestimmte Erkenntnisse, die im Rahmen der grenzpolizeilichen Kontrolle anfallen und für die Auftragserfüllung des BND als erforderlich erachtet werden.

Meine Prüfung dieses Bereichs hat ergeben, daß der BND die in den neuen Richtlinien enthaltenen Anforderungen beachtet.

3.7.4 Zur rechtlichen Eingrenzung der Datenverarbeitung des BND

Vom Gesetz zu Artikel 10 GG und den oben zu Nr. 3.7.3 erwähnten Bestimmungen abgesehen, ist nicht gesetzlich geordnet, welche Informationen der Dienst über welche Personen sammeln darf und von welchen anderen Stellen er Auskünfte erhalten soll. Die Regelungen über die Amtshilfe vermögen die Lücke nicht zu füllen, da sie im Außenverhältnis zu den Betroffenen keine ausreichende Rechtsgrundlage für die Übermittlung personenbezogener Daten an andere Stellen mit anderem Auftrag darstellen. Die Tatbestandsvoraussetzungen der allgemeinen Vorschriften des BDSG (§§ 9, 10) sind zwar insoweit erfüllt, als die Datenverarbeitung zur Erfüllung der Aufgaben erforderlich ist — was nach den Prüfungsergebnissen mit Ausnahme bestimmter Bereiche und der noch nicht bereinigten Altfälle (unten Nr. 3.7.6) im wesentlichen zutrifft —, aber da eine gesetzliche Befugnis zu Eingriffen in die Rechtssphäre der beobachteten und/oder registrierten Personen fehlt, kann im strengen Sinn nicht von „rechtmäßiger" Aufgabenerfüllung gesprochen werden. Doch waren bisher alle Forderungen nach einer gesetzlichen Regelung dieser Form staatlicher Tätigkeit erfolglos, und eine Änderung dieser Politik ist nicht zu erwarten. Bei der Bewertung dieser rechtlichen Problematik ist allerdings zu bedenken, daß der BND zu einem erheblichen Teil im Ausland und damit außerhalb unserer Rechtsordnung tätig ist.

Bei dieser Lage sollten zumindest die internen Anweisungen zur Datenverarbeitung eindeutige Grenzen ziehen. Hier bestehen jedoch noch gewisse Mängel.

Insbesondere bedürfen die Regelungen über das Personen-Dokumentationswesen im BND zum Teil noch der Präzisierung in den Punkten, die Umfang und Voraussetzungen der Speicherung und der Übermittlung betreffen. Leider wurde meine entsprechende Anregung nicht aufgegriffen. Der BND ist der Auffassung, daß die vorhandenen Regelungen ausreichend seien. Diese unterschiedliche Betrachtungsweise beruht letztlich auf einer verschiedenen Einschätzung von Generalklauseln und der unterschiedlichen Interpretation des Begriffes „rechtmäßige Aufgabenerfüllung".

Die Prüfungen der vergangenen Jahre und vor allem des Jahres 1982 haben außerdem gezeigt, daß in bestimmten Bereichen die Versuchung gegeben ist, mehr personenbezogene Daten zu speichern als bei strenger Erforderlichkeitsprüfung angebracht erscheint. Dies ist zum Teil eine Folge der vielfältigen, fast automatischen Benachrichtigungen in den verschiedenen Bereichen durch andere Sicherheitsbehörden, die wiederum überwiegend auf den in ihrer Weite kaum überbietbaren Informationsgeboten der „Richtlinien über die Zusammenarbeit in Staatsschutzangelegenheiten" i. d. F. vom 23. Juli 1973 beruhen. Es muß aber verhindert werden, daß beim BND über das unvermeidliche Mindestmaß hinaus Parallelspeicherungen zu Bereichen stattfinden, die schwerpunktmäßig zur Aufgabe der Verfassungsschutzämter und/oder Polizeien gehören.

Denn je mehr Parallelspeicherungen es gibt, um so größer wird die Gefahr, daß zu Unrecht gespeicherte oder nicht mehr erforderliche Daten unvollständig gelöscht werden. Ich habe daher zu zwei Bereichen, in denen die vorgenannte Gefahr besonders relevant erscheint, Vorschläge zu einer restriktiveren Speicherpraxis unterbreitet, die jedoch bisher nicht akzeptiert wurden. Kern der Auseinandersetzung ist die Meinungsverschiedenheit darüber, inwieweit der BND aufgrund seiner Aufgabenstellung auch Informationen speichern darf, die bei anderen Behörden, z. B. Strafverfolgungsbehörden, wegen zu geringen Bezuges zu ihren Aufgaben nicht speicherungsfähig wären.

Außerdem habe ich angeregt, das auch bei anderen Behörden praktizierte Verfahren der sog. „Zeitspeicherung" mit kürzeren Überprüfungsfristen einzuführen. In Fällen, in denen die Notwendigkeit der Speicherung für die Aufgabenerfüllung des BND nicht eindeutig feststeht, sind kürzere Fristen als die 15jährige Regelfrist angezeigt, denn die kurzfristige Überprüfung ist der unerläßliche Ausgleich für die — teilweise unverzichtbare — Speicherung von Informationen, deren Gehalt und Zuverlässigkeit ungesichert ist. Der BND hat die Praktizierung der Zeitspeicherung für die Zukunft in diesen beiden Bereichen auch zugesagt. Damit wären meine Bedenken gemildert. Darüber hinaus hat eine kurz vor Drucklegung dieses Berichts durchgeführte Ergänzungsüberprüfung in einem der vorerwähnten Bereiche gezeigt, daß der zuständige Fachbereich inzwischen eine strengere Erforderlichkeitsprüfung vornimmt, die meine Bedenken ebenfalls ausräumt.

Festzuhalten ist auch, daß der Bundesnachrichtendienst in keinem Fall Speicherungen vornimmt über Personen, zu denen an ihn lediglich eine Anfrage gerichtet wurde — beispielsweise im Zusammenhang mit einer Sicherheitsüberprüfung im Rahmen der Kabinettsrichtlinien —, wenn zu dieser Person keine eigenen relevanten Unterlagen vorhanden sind und auch im übrigen aus der Anfrage kein Grund für eine Speicherung ersichtlich ist. Die bei einer Prüfung im Laufe dieses Jahres festgestellte Ausnahme bei Anfragen des Bundeskanzleramtes ist nunmehr entsprechend meiner Anregung beseitigt.

3.7.5 Auskünfte an andere Stellen

Bei allen bestehenden Problemen muß anerkannt werden, daß Speicherungen durch den Bundesnachrichtendienst in bestimmten Bereichen auch eben unerläßlich sind. Es wäre zwar wünschenswert, wenn hier durch gesetzliche Regelungen die erforderliche Klarheit geschaffen würde. Dies ist aber wohl auf absehbare Zeit nicht zu erreichen. Dann muß aber zumindest das Auskunftsverhalten in solchen Bereichen, in denen personenbezogene Datenverarbeitung unerläßlich erscheint, die erforderlichen Rechtsgrundlagen hierfür jedoch fehlen, besonders restriktiv gestaltet werden. Denn meist ist nicht die Speicherung als solche das Problem, sondern die Übermittlung an andere Stellen zu anderen Verfahren.

Ich habe deshalb zu verschiedenen Tätigkeitsbereichen des BND angereget, daß jeweils eine restriktivere Auskunftspraxis gewählt wird. Dabei besteht Einigkeit darüber, daß dies nicht gelten kann, wenn es um die Aufklärung oder Verhütung schwerer Straftaten geht.

Nicht selten ist beim BND — aber auch bei anderen Sicherheitsbehörden — eine Speicherung allein darauf zurückzuführen, daß eine andere Dienststelle eine Meldung über die Einleitung eines Verfahrens oder über das Bestehen eines Verdachts gemacht hat. Ist der weitere Gang dieses Verfahrens, die Bestätigung oder Widerlegung des Verdachts der speichernden Stelle nicht bekannt, so muß vor einer Auskunft an dritte Stellen geprüft werden, ob die Speicherung noch relevant ist und ob eine Auskunft über den ursprünglichen Tatbestand verantwortet werden kann. Dazu muß der Ausgang des Verfahrens oder die weitere Aufklärung der ursprünglichen Verdachtsmomente bei der meldenden Stelle erfragt werden. Bisher war dies beim BND offenbar nicht so gehandhabt worden, wie die Prüfung eines Einzelfalles und die Erörterungen hierzu mit den Vertretern des BND ergeben haben. Es ist vorab zu betonen, daß dies der bisher einzige *festgestellte* Fall dieser Art ist. Wenn er dennoch hier dargestellt wird, so deshalb, weil er die bisherige Rechtsauffassung des BND deutlich macht:

Im Jahre 1963 war zu einer bestimmten Person eine Akte angelegt worden, weil von zwei Staatsanwaltschaften Hinweise auf die Verwicklung der Person in ein Verfahren mit nachrichtendienstlichem Hintergrund gegeben worden waren. (An der materiellen Erforderlichkeit zur Anlegung der Akte *zu diesem Zeitpunkt* besteht kein Zweifel.) Zu dieser Person wurde 18 Jahre später, im Jahre 1981, von einer anderen Sicherheitsbehörde Auskunft erbeten. Die Akte war in der Zwischenzeit nicht überprüft und auch nicht mehr ergänzt worden. Der Hinweis aus dem Jahre 1963 war somit nach wie vor der einzige Grund für die Speicherung der Akte. Deshalb hätte nunmehr sowohl nach den eigenen Löschungsrichtlinien des BND als auch nach dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit nachgeprüft werden müssen, ob die Speicherung für den BND überhaupt noch Relevanz hat und ob demgemäß eine Auskunft nach so langer Zeit noch erfolgen darf. Hierzu wäre eine Nachfrage über den Ausgang des Verfahrens bei den ursprünglich meldenden Dienststellen erforderlich gewesen. Diese unterblieb. Statt dessen wurde die Speicherung ohne nähere Prüfung aufrechterhalten, und es wurde Auskunft über den Hinweis aus dem Jahre 1963 erteilt.

Die Vertreter des BND waren der Auffassung, hier richtig gehandelt zu haben. Man habe nur unter Angabe des Aktenzeichens mitgeteilt, daß der Betroffene in einem Ermittlungsverfahren bei zwei Staatsanwaltschaften „in Erscheinung getreten" sei (dies ist richtig), also nur auf Erkenntnisse anderer Behörden verwiesen, und es sei allein Aufgabe der empfangenden Stelle, derartige Hinweise nachzuprüfen, bevor eine Verwertung nach außen gegen-

über dem Bürger erfolge. Genau in dieser grundsätzlichen Haltung liegt das Problem.

Die Rechtsauffassung des BND ist jedoch m. E. nicht richtig. Die unüberprüfte Aufrechterhaltung einer Speicherung und unüberprüfte Auskunft nach Ablauf einer so langen Zeit stellt m. E. einen Verstoß gegen die Prinzipien der §§ 9 und 10 BDSG (Zulässigkeitsvoraussetzungen für Speicherung und Übermittlung personenbezogener Daten) in Verbindung mit dem Grundsatz der Verhältnismäßigkeit dar. Da der BND in besonderen Fällen zur Auskunft an andere Sicherheitsbehörden verpflichtet ist, besteht bei einem solchen Verhalten die Gefahr, daß unüberprüfter Verdacht weiter gestreut, somit weiter aufrechterhalten und auch gegenüber dem Bürger verwertet wird. Zwar muß auch die empfangende Stelle die Relevanz der Daten vor einer Verwertung gegenüber dem Bürger selbst überprüfen. Aber dies entbindet die übermittelnde Stelle jedenfalls nach Ablauf einer so langen Zeit und nach Überschreiten der eigenen Löschungsfristen nicht von der eigenen Prüfungspflicht.

Erfreulicherweise haben sich die Vertreter des BND inzwischen bereit erklärt, die Staatsanwaltschaften, die dem BND Hinweise auf eingeleitete Verfahren geben, auch jeweils um Meldung des Verfahrensausgangs zu bitten. Soweit dies nicht geschieht, hat der BND zugesagt, bei fremden Verfahren wenigstens nach Ablauf von 15 Jahren in der Regel nur dann Auskunft zu erteilen, wenn vorher durch Rückfrage der Ausgang des Verfahrens und damit gleichzeitig die Notwendigkeit weiterer Speicherung geklärt ist.

Ich halte jedoch diesen Kompromiß noch nicht für ausreichend. Vielmehr sollte die gleiche Prüfungspflicht in allen Fällen gelten, in denen Hinweise von anderen Stellen gegeben werden, die einen Verdacht betreffen, der noch nicht endgültig aufgeklärt ist. Es erscheint auch nicht als angemessener Lösungsweg, auf eine eigene und aus Rechtsgründen erforderliche Relevanzprüfung vor der Auskunftserteilung zu verzichten und statt dessen nur einen Hinweis auf die ursprünglich meldende Stelle statt einer inhaltlichen Auskunft zu geben. Dies kann allenfalls ein Notbehelf in besonders gelagerten Fällen sein, wie ich oben zu 3.2.2 (S. 80) näher dargelegt habe.

3.7.6 Bereinigung der Altfälle

Meine Prüfungen in diesem Jahr haben ergeben, daß beim BND zur Zeit noch eine große Anzahl von Personen registriert ist, die über 70 Jahre alt sind und bei denen die Speicherwürdigkeit überprüft werden müßte. Zu bereinigen sind auch diejenigen Vorgänge, in denen seit 15 Jahren nichts mehr ergänzt wurde. Eine solche Auswertung ist jedoch aus datentechnischen Gründen nicht automatisiert möglich, da das Erfassungsdatum noch nicht so lange gespeichert wird. Selbst wenn man hiervon den Personenkreis abzieht, der — wie die Mitarbeiter des BND — verständlicherweise nicht unter die Fristenregelung fällt, dürfte noch eine erhebliche Zahl verbleiben.

Aufgrund der besonderen organisatorischen Regelung des Auskunftswesens sind die Gefahren von Fehlübermittlungen und weiteren Fehlentscheidungen anderer Behörden im Hinblick auf solche weitgehend nicht mehr relevanten Speicherungen dann gering, wenn hierfür eine Auskunftssperre verhängt wird. Dies ist notwendig, solange es — wie bisher — nicht möglich ist, alle Fälle schnell abzuarbeiten.

Die Auskunftssperre sollte stets dann gelten, wenn es sich um Personen handelt, die über 70 Jahre alt sind *und* deren Datensätze mehr als 15 Jahre nicht bewegt wurden. Ausnahmen hiervon sind nur in besonderen Fällen zulässig (vgl. oben Nr. 3.2.3).

3.7.7 Zusammenfassung

Die vorstehenden Ausführungen haben auf eine Reihe von Problemen sowie auf Verfahrensweien des BND hingewiesen, die bedenklich, inzwischen aber durch die erwähnten Vereinbarungen weitgehend abgebaut sind. Es ist andererseits hervorzuheben, daß unabhängig von den getroffenen Vereinbarungen und meinen Anstößen auch seitens des BND ein fortgesetztes Bemühen um Beachtung datenschutzrechtlicher Erfordernisse erkennbar ist. Dabei stimmt das Datenschutzinteresse im Ergebnis oft mit eigenen Sicherheitsbedürfnissen überein.

So konnte ich z. B. jedenfalls bisher bei meinen Prüfungen feststellen, daß nur selten gegen Richtlinien verstoßen wurde. Zusagen waren immer eingehalten und umgehend durchgeführt worden. Das gilt insbesondere für die Löschungen, die anläßlich meiner Prüfungen vereinbart wurden.

Die Prüfung der seit 1. Dezember 1981 praktizierten neuen Amtshilferichtlinien zwischen BGS und BND hat ebenfalls gezeigt, daß die darin enthaltenen verfahrensrechtlichen Sicherungen mit besonderen Anforderungen an Auswertung, Speicherung usw. vom BND von Anfang an beachtet wurden und werden.

Das Löschungsverfahren ist beim BND in einer Weise geregelt, die als vorbildlich bezeichnet werden muß. Allerdings ist der verfahrensmäßige Ablauf nur die eine Seite. Entscheidend ist natürlich, ob auch im erforderlichen Umfang Daten, die nicht mehr relevant sind, wirklich gelöscht werden. Bisher war das nicht der Fall, wie oben zu Nr. 3.7.6 dargelegt. Sobald jedoch die vereinbarten Verbesserungen durchgeführt werden (insbesondere die Nachfrage nach dem Ausgang eines relevanten Verfahrens etc.), kann dieser Mangel als beseitigt gelten. Daß es daneben gelegentlich zu Fehlern in Einzelfällen kommt, läßt sich nie gänzlich vermeiden und ändert nichts an der Qualität der Regelungen.

3.8 Zollkriminalinstitut

3.8.1 Stand der Datenverarbeitung beim Zollkriminalinstitut

Das Zollkriminalinstitut ist Teilnehmer des Informationssystems für den Zollfahndungsdienst (IN-

ZOLL). Dieses System wird auf der Basis der Straftaten/Straftäter-Datei beim Bundeskriminalamt betrieben. Zugriff auf dieses System haben neben dem Zollkriminalinstitut die Zollfahndungsämter. Im INZOLL sind neben den Personendaten umfangreiche Fallhinweise über das begangene Zoll- oder Verbrauchsteuerdelikt erfaßt. Das Zollkriminalinstitut stellt außerdem Personengrunddaten und Bearbeitungshinweise in das Informationssystem der Polizei, Bereich polizeiliche Beobachtung, ein. In einer manuellen Kartei werden außerdem Personengrunddaten und Fundstellenhinweise auf beim Zollkriminalinstitut vorhandene Vorgänge gespeichert.

3.8.2 Kontrolltätigkeit

Datenschutzrechtliche Kontrollen konnten im vergangenen Jahr im Zollkriminalinstitut (ZKI) nicht durchgeführt werden. Da das ZKI in Übereinstimmung mit dem Bundesminister der Finanzen (BMF) der Auffassung ist, daß das Steuergeheimnis meiner Prüfkompetenz entgegensteht, konnte ich lediglich anhand einer einzigen Eingabe eine Einzelprüfung vornehmen. Ich kann deshalb über die Einhaltung des Datenschutzrechts im Bereich des Zollkriminalinstituts nicht berichten.

3.8.3 Zollrechtliche Überwachung

Hingegen ergibt sich nach meiner Auffassung aus dem mit dem Bundesminister der Finanzen geführten Schriftwechsel, daß im Bereich der Zollrechtlichen Überwachung (ZÜ) nach wie vor gegen Datenschutzrecht, insbesondere gegen das in der Abgabenordnung (AO) geschützte Steuergeheimnis verstoßen wird.

Im Jahre 1980 wurde nach Kritik am bis dahin geübten System der „beobachtenden Fahndung" („Befa") eine neue Polizeidienstvorschrift (PDV) 384.2 erlassen. Die Voraussetzungen für die Einstellung in die polizeiliche Beobachtung wurden verschärft. Erfaßt werden dürfen seitdem nur noch gefährliche Intensivtäter sowie Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, daß sie als Täter einer Reihe im einzelnen in der PDV 384.2 aufgeführter, schwerer Straftaten in nicht unerheblichem Umfang tätig sind. Will das Bundeskriminalamt eine Person zur polizeilichen Beobachtung zum Zwecke der Strafverfolgung ausschreiben, so holt es das Einverständnis der Staatsanwaltschaft ein, es sei denn, es ist Gefahr im Verzug. Daneben gibt es noch die Möglichkeit, Personen unter bestimmten Voraussetzungen im Rahmen der Führungsaufsicht zur Beobachtung auszuschreiben.

Zugleich wurde 1980 in Ziffer 4 der PDV 384.2 das neue Instrument der zollrechtlichen Überwachung eingeführt. Die Voraussetzungen für die Ausschreibung einer Person zur ZÜ sind weiter gefaßt als die Voraussetzungen für die Ausschreibung zur polizeilichen Beobachtung. Es können ausdrücklich auch solche Personen ausgeschrieben werden, bei denen zwar bisher noch nicht ausreichende tatsächliche Anhaltspunkte, wohl aber die begründete Vermutung besteht, daß sie im Rahmen des grenzüberschreitenden Verkehrs in nicht unerheblichem Umfang als Schmuggler auftreten bzw. zu Schmuggelzwecken eingesetzt werden. Eine Beteiligung der Staatsanwaltschaft ist hier nicht vorgesehen.

Diese im Vergleich zur polizeilichen Beobachtung geringeren Voraussetzungen zur Ausschreibung rechtfertigen sich daraus, daß auch die Konsequenzen unterschiedlich sind. Die polizeiliche Beobachtung kann zur Erstellung eines Bewegungsbildes einschließlich der Begleitpersonen etc. führen. Aufgrund der Ausschreibung zur ZÜ dürfen keinerlei polizeiliche Maßnahmen ergriffen werden, sondern nur zollrechtliche Maßnahmen, d. h. in der Praxis die an der Grenze üblichen Zollkontrollmaßnahmen.

Derartige Zollkontrollmaßnahmen dürfen nur von Zollbeamten und unter bestimmten Voraussetzungen von BGS-Beamten vorgenommen werden. Gleichwohl sind die zur ZÜ ausgeschriebenen Personen im allgemeinen Fahndungssystem der Polizei INPOL erfaßt. Der Bundesminister der Finanzen hat mir mit Schreiben vom 3. November 1982 zwar mitgeteilt, daß die Hausinspektion des Deutschen Bundestages, die Bahnpolizei und der Fahndungsdienst der Bundesbahn künftig keinen Zugriff auf Daten aus der ZÜ mehr haben sollen. Es bleiben aber ca. 2 500 Polizeidienststellen, die nach wie vor über diesen Zugriff verfügen. Diesen Polizeidienststellen gegenüber sind, weil jederzeit abrufbar, Steuerdaten derjenigen offenbart, die zur zollrechtlichen Überwachung ausgeschrieben sind. Der Bundesminister der Finanzen ist der Auffassung, daß das Steuergeheimnis nach § 30 AO in diesem Fall nicht verletzt ist, weil jedenfalls in Fällen des vermuteten Rauschgift- und Waffenschmuggels die Offenbarung der Steuerdaten nach § 30 Abs. 4 Nr. 5 AO ausnahmsweise zulässig sei.

Nach dieser Vorschrift dürfen Steuerdaten offenbart werden, wenn hierfür ein zwingendes öffentliches Interesse besteht. Waffen- und Rauschgiftschmuggel sind schwere Straftaten, an deren Verfolgung ein erhebliches öffentliches Interesse besteht. Es besteht aber nach meiner Auffassung kein zwingendes öffentliches Interesse gerade an der generellen Offenbarung der in diesem Zusammenhang anfallenden Steuerdaten gegenüber der Polizei. Gerade dies wäre aber die Voraussetzung, unter der allein die Ausnahmevorschrift des § 30 Abs. 4 Nr. 5 AO eingreifen würde. Da nach der PDV 384.2 gegenüber den zur ZÜ ausgeschriebenen Personen nur zollrechtliche Maßnahmen ergriffen werden dürfen und die Durchführung strafprozessualer oder polizeirechtlicher Eingriffsmaßnahmen sogar ausdrücklich untersagt ist, ist nicht einsehbar, weshalb Behörden von einer Ausschreibung zur ZÜ Kenntnis gegeben werden soll, die nicht nur mit zollrechtlichen Maßnahmen nichts zu tun haben, sondern denen auch Maßnahmen allein aufgrund der Ausschreibung in der ZÜ nach eigenen Kompetenzvorschriften nicht erlaubt sind. Die Übermittlung der Daten der zur ZÜ ausgeschriebenen Personen an die an INPOL angeschlossenen Polizeibehörden ist also überflüssig, in jedem Falle aber be-

steht an dieser Übermittlung kein zwingendes Interesse, wie es allein gemäß § 30 Abs. 4 Nr. 5 AO eine Durchbrechung des Steuergeheimnisses rechtfertigen könnte.

Der Bundesminister der Finanzen hat mir in seinem Schreiben vom 3. November 1982 nunmehr mitgeteilt, daß die Fälle der ZÜ, die nicht Waffen- und Rauschgiftschmuggel betreffen, in Zukunft nur noch den Terminals an der Grenze zugänglich sein sollen. Dies ist eine Konsequenz, die sich aus dem in § 30 AO geschützten Steuergeheimnis ergibt und die ich seit langem fordere.

Nicht konsequent ist es hingegen aus den vorgenannten Gründen, wenn Rauschgift- und Waffenschmuggel-Fälle aus der ZÜ weiterhin automatisch an alle Polizeidienststellen übermittelt werden. Hier bleibt es nach meiner Ansicht beim Verstoß gegen § 30 AO und der damit verbundenen Verletzung des Steuergeheimnisses. Wenn Beobachtungsfälle aus den Verdachtsbereichen Rauschgift- und Waffenschmuggel den inländischen Polizeibehörden bekanntgegeben werden sollen, so bleibt nach meiner Auffassung nur der Weg der Ausschreibung zur polizeilichen Beobachtung. Im Rahmen der polizeilichen Beobachtung ist eine Ausschreibung zur Beobachtung in den Deliktsbereichen Rauschgift- und Waffenschmuggel möglich. Das ZKI ist sogar selbst befugt, solche Ausschreibungen vorzunehmen. Es müssen dann aber die oben skizzierten — gegenüber der ZÜ strengeren — Voraussetzungen vorliegen. Darüber hinaus erstatten die Zolldienststellen über jeden entdeckten Fall von Rauschgift- oder Waffenschmuggel eine Sofortmeldung an die Polizei. Wenn die Polizei dem ZKI solche Fälle übermittelt, in denen die Voraussetzungen zur polizeilichen Beobachtung nicht ausreichen, wohl aber zur zollrechtlichen Überwachung, so läßt dies den Schluß zu, daß hier jedenfalls für einen Teilbereich die mit der Einführung der PDV 384.2 erreichten rechtsstaatlichen Verbesserungen im Ergebnis nicht zum Tragen kommen. Ob nämlich eine Person zu der (jetzt nur noch unter engeren Voraussetzungen zulässigen) polizeilichen Beobachtung oder zur (nach wie vor unter weiten Voraussetzungen zulässigen) ZÜ ausgeschrieben wird, bleibt von den Wirkungen her solange gleich, wie die inländischen Polizeidienststellen Zugriff auf die ZÜ, zumindest auf deren wichtigste Bereiche Rauschgift- und Waffenschmuggel, haben.

Im vorstehenden ist geschildert, daß jedenfalls objektiv im Bereich der Rauschgift- und Waffenschmuggeldelikte die Möglichkeit besteht, die rechtsstaatlichen Sicherungen der PDV 384.2 zu unterlaufen. Ob von dieser Möglichkeit auch Gebrauch gemacht wird, kann ich nicht endgültig beurteilen, da mir der Bundesminister der Finanzen und das Zollkriminalinstitut eine systematische Kontrolle der ZÜ unter Berufung auf das Steuergeheimnis verwehrt haben.

3.9 Kreiswehrersatzämter

Bei verschiedenen Kreiswehrersatzämtern wurden die Fachgebiete, die für die personelle Bedarfsdeckung nach dem Wehrpflichtgesetz, die Musterung der Wehrpflichtigen, den ärztlichen Dienst, den psychologischen Dienst und den Berufsförderungsdienst zuständig sind, ferner die Prüfungsausschüsse, die über die Anträge auf Anerkennung als Kriegsdienstverweigerer entscheiden, ein Wehrdienstberater und ein Bundesgrenzschutzberater beraten und kontrolliert. Schwerpunkt dieser Kontrollen waren die technischen und organisatorischen Maßnahmen zur Sicherung der Datenverarbeitung.

Zum Geschäftsbereich des Bundesministers der Verteidigung gehören 97 Kreiswehrersatzämter. Alle Kreiswehrersatzämter haben prinzipiell die gleiche Organisation, aber nicht alle haben die gleichen Aufgaben zu erfüllen. Zusammen mit dem Bundesminister der Verteidigung wurden die Kontrollen bei den Kreiswehrersatzämtern vorbereitet insbesondere mit dem Ziel, am Beispiel der Aufgabenerfüllung in mindestens einem großen, einem mittleren und einem kleinen Kreiswehrersatzamt zu zeigen, welche technischen und organisatorischen Maßnahmen erforderlich sind, um den Datenschutz im Kreiswehrersatzamt zu gewährleisten. An den Kontrollen selbst nahmen stets Vertreter des Bundesministers der Verteidigung und der die Fachaufsicht über das Kreiswehrersatzamt ausübenden Wehrbereichsverwaltung teil. Dieses gemeinsame Vorgehen hat sich bewährt und führte in einigen Fällen dazu, daß von mir entdeckte Mängel sofort beseitigt wurden.

Die Ergebnisse aus allen Kontrollbesuchen und den dabei erfolgten Einzelberatungen wurden zusammen mit dem Bundesminister der Verteidigung aufgearbeitet. Dabei zeigten sich keine Divergenzen in der Beurteilung der aufgedeckten Mängel und der als notwendig erkannten Maßnahmen:

a) Bei einer Vielzahl von Kreiswehrersatzämtern wurden Karteien über Wehrpflichtige, die aus dem Zuständigkeitsbereich des jeweiligen Kreiswehrersatzamtes verzogen waren, vernichtet. Diese Karteien wurden seit Einführung des automatisierten Verfahrens zur Wehrüberwachung nicht aktualisiert, sie wurden lediglich aufbewahrt.

b) Im Fachgebiet „Psychologischer Dienst" wird neu geregelt, wie die sogenannten Arbeitskarten mit den Ergebnissen der Eignungs- und Verwendungsprüfung aufbewahrt und wie Überschreitungen der vorgeschriebenen Aufbewahrungsfristen sicher verhindert werden.

c) Die Organisation der Verwaltung der Prüfungsausschüsse für die Anerkennung von Kriegsdienstverweigerern (KDV) wird neu geregelt werden. Vorrangig wird das Volumen der Daten reduziert werden, mit denen ein Antrag auf Kriegsdienstverweigerung im sogenannten KDV-Register beschrieben wird. Dieses Register wird geführt, um den ordnungsgemäßen Ablauf eines KDV-Antrages überwachen zu können. Hierfür sind nur wenige Angaben erforderlich (z. B. Datum des Eingangs des Antrags, Aktenzeichen, Name des Wehrpflichtigen, Datum der

Abgabe an den Prüfungsausschuß). Um jedoch auch den zahlreichen Wünschen nach statistischen Auswertungen über Kriegsdienstverweigerer nachkommen zu können, werden viele zusätzliche Daten registriert (z. B. Beruf, Schulbildung) und der gesamte Ablauf eines Verfahrens bis hin zur Revision und sonstige Gründe der Erledigung dargestellt. Weil die Statistiken gelegentlich zurückliegende Zeiträume mit umfassen sollen, werden diese Register zum Teil sehr lange aufbewahrt. Es gilt, hier ein Verfahren zu finden, das die schutzwürdigen Belange der Kriegsdienstverweigerer wahrt und zugleich den Informationsbedürfnissen des Parlaments über diese Personengruppe entgegenkommt. Ich habe hierzu meine Beratung angeboten.

d) In einzelnen der kontrollierten Kreiswehrersatzämter wurden nicht erforderliche Datensammlungen vorgefunden. Sie wurden inzwischen aufgelöst oder vernichtet; nicht mehr benötigte Unterlagen wurden an das Militärarchiv abgegeben oder die Termine zur Löschung neu bestimmt.

e) Die Fachaufsicht der Kreiswehrersatzämter wird künftig verstärkt prüfen, ob die jeweilige Handhabung der Vorschriften in den einzelnen Kreiswehrersatzämtern auch den Datenschutz gewährleistet. Die Leiter der Kreiswehrersatzämter werden sorgfältig erheben oder erheben lassen, wie die Datenverarbeitung in den einzelnen Arbeitsgängen in ihrer Behörde tatsächlich erfolgt, und damit den Anforderungen an die Übersicht gemäß § 15 BDSG, wie ich sie empfehle, nachkommen.

Hervorheben möchte ich, daß in einem der kontrollierten Kreiswehrersatzämter im süddeutschen Raum die Datenverarbeitung so zweckmäßig und geradlinig organisiert war, daß sowohl Aufgabenverteilung als auch Gewährleistung des Datenschutzes als vorbildlich bezeichnet werden können.

4 Nicht-öffentlicher Bereich

4.1 Adreßhandel

Viele Bürger sind an Werbung interessiert, für manche ist sie ein Stein des Anstoßes. Der Datenschutz interessiert sich für Werbemaßnahmen nur, wenn der einzelne Bürger gezielt angesprochen wird, wenn also das werbende Unternehmen über Informationen verfügt, die es aus seiner Sicht lohnenswert erscheinen lassen, gerade diesem Betroffenen ein Angebot zu unterbreiten. Solch eine zielgerichtete Werbung kann für den Werbungtreibenden wie für den Umworbenen nützlich sein. Sie kann aber als aufdringlich und verletzend empfunden werden, wenn sie an sehr persönliche Umstände anknüpft, z. B. Angaben ausnutzt, die man einem Institut für Partnervermittlung anvertraut hat.

Ich berichte über diesen Bereich privater Datenverarbeitung, der außerhalb meiner Kontrollzuständigkeit liegt, deshalb, weil das Gesetz die Aufsichtsbehörden der Länder nicht verpflichtet hat, über ihre Erfahrungen der Öffentlichkeit zu berichten.

Die nach wie vor bei mir eingehenden Beschwerden zeigen, daß viele Bürger sich gerade beim Adreßhandel persönlich mit dem Datenschutz auseinandersetzen möchten. Sie klagen zum einen über verstopfte Briefkästen, zum anderen haben sie Bedenken dagegen, daß Erkenntnisse über sie gesammelt und — sei es auch nur zu Werbezwecken — ausgewertet oder sogar verkauft werden.

Darin liegt der eigentlich datenschutzrelevante Aspekt der Direktwerbung. Für den Betroffenen unmittelbar erkennbar ist meist nur die Verwendung seiner Anschrift. Wie der Begriff „Direktwerbung" schon sagt, wendet sich der Werbende „direkt" und damit zielgerichtet an eine bestimmte Person, von der er weiß oder annimmt, daß sie Interesse an seinen Angeboten hat. Dazu braucht er Informationen über sie, also je nach dem Ziel der Werbemaßnahme Angaben über Einkommens- und Vermögensverhältnisse, Hobbys, Neigungen, Interessen, Beruf. Wer also Anschriften für die Direktwerbung benötigt, wählt unter Zugrundelegen bestimmter Aspekte aus. Bei der Weitergabe von Anschriften ist dieser Gesichtspunkt der damit verbundenen Weitergabe von Zusatzinformationen über den Betroffenen zu bedenken. Dies wird aber von einigen Unternehmen bisher nicht berücksichtigt.

Weiterhin muß man zur Kenntnis nehmen, daß die Zusatzinformationen vielfach ungenau und mitunter falsch sind. So wird aus einer einmaligen Bestellung einer Ware auf Neigungen und Hobbys geschlossen, obwohl es sich um ein Geschenk gehandelt haben kann. Die Zugehörigkeit zu einer bestimmten Einkommensklasse veranlaßt Werbetreibende immer wieder, die Betroffenen als Interessenten für spekulative Geldanlagen anzuschreiben.

Wenn mit solchen unzutreffenden Zusatzinformationen gehandelt wird, dann kann das schutzwürdige Belange der Betroffenen berühren. Vor diesem Hintergrund ist die Diskussion um die Weitergabe von Daten für Werbezwecke zu beurteilen.

Die öffentliche Verwaltung kann — abgesehen von der Bundespost (siehe oben Nr. 2.5.4) — als Datenquelle kaum mehr in Anspruch genommen werden. Behörden erteilen Gruppen- und Massenauskünfte in der Regel nur noch mit Einwilligung der Betroffenen. Soweit die Adreßwirtschaft ihr Datenmaterial allgemein zugänglichen Quellen wie dem Telefon- und dem Adreßbuch entnimmt, ist dies datenschutzrechtlich unproblematisch. Etwas anderes gilt, wenn sich der Adreßhandel darüber hinaus als Vermittler betätigt (sogenannes List-Broking), er also Anbieter und Nachfrager von Anschriften zusammenführt und eventuell im Auftrag beider Seiten die Werbemaßnahme durchführt (als sogenannter Letter-Shop). Dann trifft das oben Gesagte über die Weitergabe der Zusatzinformationen wieder zu, und der Adreßhändler trägt als (guter) Makler bei diesem Geschäft eine Mitverantwortung für die datenschutzgerechte Abwicklung.

Diese Fallgestaltung der Vermittlung und Vermietung von Anschriften ist beim Adreßhandel sehr verbreitet. Für den Betroffenen ist es zunächst gleichgültig, wer bei dem Werbegeschäft welchen Teilvorgang bearbeitet. Er muß aber in die Lage versetzt werden, seine datenschutzrechtlichen Ansprüche auf Auskunft, Berichtigung, Sperrung und Löschung durchsetzen zu können. In der Praxis scheitert dies in der Regel daran, daß sich der Betroffene — verständlicherweise — damit an das werbende Unternehmen wendet. Dieses erfährt aber erstmalig aufgrund der Reaktionen von Betroffenen, welche Personen angeschrieben wurden.

Welche Stellen die Datenverarbeitung vornehmen, kann der Betroffene nicht in Erfahrung bringen, da er keinen dahin gehenden Auskunftsanspruch hat.

Beim Handel mit Adressen zeigen sich somit deutlich zwei Mängel: erstens die fehlende Berücksichtigung der Tatsache, daß bei der Weitergabe von Adressen für die Direktwerbung Zusatzinformationen über den Betroffenen die wesentliche Rolle spielen, und zweitens das fehlende Wissen, wer verantwortlich über die Daten verfügt.

Nachdem die beiden oben genannten Probleme zwischen den Datenschutzaufsichtsbehörden und der Adreßwirtschaft diskutiert waren, hat ein namhaftes Adreßhandelsunternehmen in Werbeschreiben die Gründe für die Auswahl der Anschrift erläutert sowie einen Hinweis auf die Datenquelle gegeben.

Ein norddeutsches Spezialunternehmen, das Kundenanschriften vermietet, klärt darüber seine Kunden auf und gibt durch einen entsprechenden Passus auf dem Bestellformular die Möglichkeit, die Vermietung auszuschließen. Zu Geschäftseinbußen hat das nicht geführt. Weniger als 2 % der Kunden entscheiden sich für eine Datensperre. Alle Unternehmen, die diese Form der Verbraucheraufklärung in der Bundesrepublik Deutschland bereits getestet haben bzw. praktizieren, berichten über gute Erfahrungen.

Aus den USA wird berichtet, daß rund 300 namhafte Versandhäuser, Verlage und andere im Direkt-Marketing tätige Unternehmen diese Form der Aufklärung vornehmen.

Mir scheint mit mehr Transparenz in der Direktwerbung eine datenschutzgerechte und zweckmäßige Lösung gefunden zu sein. Auf der einen Seite wird der Betroffene über das Verfahren aufgeklärt und kann seine persönliche Entscheidung treffen, ob er auf die Werbung antwortet und damit dem werbenden Unternehmen auch das Zusatzwissen indirekt bekanntgibt, auf der anderen Seite wird die Direktwerbung als eine Möglichkeit rationeller wirtschaftlicher Betätigung nicht behindert.

Ich schlage daher als gesetzgeberische Maßnahme vor, daß jede Stelle, die eine Anschrift aus fremder Quelle benutzt, verpflichtet wird, die Datenquelle bekanntzugeben sowie darüber aufzuklären, unter welchen Gesichtspunkten die fremdbezogene Adresse ausgewählt wurde. Soweit es nicht möglich ist, die Datenquelle anzugeben, weil entweder keine Aufzeichnungen darüber bestehen, welche Anschrift aus welchem Datenbestand entnommen wurde, oder weil das werbende Unternehmen die gesamte Datenverarbeitung als Auftrag vergeben hat, sollten zumindest folgende Erläuterungen im Werbeschreiben enthalten sein: im ersten Fall die Angabe der in Frage kommenden Firmen, deren Anschriften genutzt wurden; im zweiten Fall eine Beschreibung, wie die Werbeaktion abgewickelt wurde und welche Stelle datenschutzrechtlich verantwortlich ist.

4.2 Handels- und Wirtschaftsauskunfteien

Handels- und Wirtschaftsauskunfteien werden häufig bei Geschäftsvorgängen mit finanziellem Risiko (z. B. Kreditvergabe, Teilzahlungskauf, Lieferung gegen Rechnung) eingeschaltet, um vor einem Geschäftsabschluß die Kreditwürdigkeit des Kunden zu überprüfen. Ich habe die Zusammenhänge ausführlich in der Broschüre „Der Bürger und seine Daten“, eine Information zum Datenschutz, S. 55f. dargestellt.

Die Aufgabe des Datenschutzes besteht in diesem Bereich darin, die Datenverarbeitung durch Handels- und Wirtschaftsauskunfteien für den Betroffenen transparent zu machen, die Vorgehensweise bei Datenrecherchen einzugrenzen, den Umfang der Daten auf entscheidungsrelevante bzw. aus den Sachverhalten abzuleitende Bewertungen zu beschränken und nur nachweisbar „richtige“ Daten zu verwenden.

Ein wichtiger Gegenstand der Verhandlungen zwischen den Datenschutzaufsichtsbehörden und der Kreditwirtschaft war die sogenannte Schufa-Klausel (vgl. 1. TB S. 42). Obwohl wesentliche Verbesserungen durch Präzisierungen und Klarstellungen in der neu formulierten Klausel erreicht werden konnten (vgl. 2. TB S. 55), ist der gefundene Kompromiß aus der Sicht des Datenschutzes nicht zufriedenstellend. Die Aufklärung über die Zusammenarbeit der Kreditwirtschaft mit der Schufa beschränkt sich auf den Hinweis, daß Daten bei der Schufa gespeichert werden. Die entscheidende Wirkung der Schufa geht jedoch von der Auskunftsbereitschaft, d. h. von den Datenübermittlungen an andere Stellen aus. Die gebotene Klarstellung war leider bisher nicht durchzusetzen.

Im Bereich der Handels- und Wirtschaftsauskunfteien haben sich die Aufsichtsbehörden mit einer Vielzahl von Problemen beschäftigt, die teilweise mit den geltenden Bestimmungen nicht befriedigend gelöst werden konnten. So paßt beispielsweise die Begrenzung des BDSG auf dateimäßige Datenverarbeitung nicht zu den Verhältnissen vieler Auskunfteien; die Entgeltregelung wurde mitunter mißbräuchlich zur Abschreckung von Auskunftsbegehren benutzt; die vorgeschriebene Benachrichtigung verwendete man nicht selten dazu, durch geschickte Formulierungen eine Selbstauskunft des Betroffenen zu erhalten; Auskunftbegehren wurden schleppend bearbeitet; Korrektur- und Löschungsansprüche versuchte man auf andere Stellen abzuwälzen; es wurde über den Umfang des Auskunftsanspruchs gestritten: Bezieht er sich nur auf den sogenannten Datenspiegel oder auf alle der Auskunftei vorliegenden Informationen? Fallen auch Archivbestände unter die Auskunftspflicht? Hat der Betroffene einen Anspruch auf Bekanntgabe der Datenquelle sowie der Empfänger von Datenübermittlungen? Weiterhin wurde darüber diskutiert, ob Löschungsfristen, die für andere Datenbestände, z. B. das Schuldnerverzeichnis, gelten, auf die Dauer der Speicherung bei Auskunfteien übertragbar sind.

Die ungelösten Probleme ließen es erwägenswert erscheinen, eine spezialgesetzliche Regelung anzustreben (vgl. 2. TB S. 58f.). Diese Empfehlung hat die Bundesregierung bisher nicht aufgegriffen.

In der Zwischenzeit wurden für eine Reihe von Fragen Lösungen entwickelt, zum Teil in Zusammenarbeit mit den davon betroffenen Unternehmen und Wirtschaftsverbänden. Als Beispiel möchte ich die im Jahre 1981 zwischen den obersten Aufsichtsbehörden — zusammengefaßt im „Düsseldorfer Kreis“ — und Vertretern der Wirtschaftsauskunfteien abgestimmten Festlegungen und Verfahrensweisen erwähnen. Dazu gehören u. a.:

— Regelungen zur Nachbarschaftsbefragung: Reduzierung dieser Art von Recherche auf wenige Fälle, Beschränkung in den restlichen Fällen auf Angaben über Wohnort/Aufenthaltsdauer, Ein-

kommen, Arbeitgeber, wirtschaftliche Verhältnisse/Bankverbindung.

— Beschränkung persönlicher Beurteilungen auf positive Feststellungen. Die empfohlene Formulierung lautet: „Aufgrund der hier aufgeführten Tatsachen wird der Betroffene positiv beurteilt."

— Beschränkung der Übermittlung von Schätzdaten auf Angaben über Alter, Einkommen, Betriebszahlen, Grundstückswert. Schätzgrundlagen und -methoden sind gegebenenfalls offenzulegen.

— Übermittlungen an Arbeitgeber aus Anlaß von beabsichtigten Personaleinstellungen nur, soweit dies wegen der speziellen Verwendung des Mitarbeiters von wirtschaftlicher Bedeutung ist (z. B. Kassierer, Geldbote).

— Bekanntgabe der Datenquelle, wenn der Nachweis erbracht wird, daß der Betroffene die Information zur Verfolgung seiner Rechte benötigt.

Außerdem ist festzustellen, daß eine Reihe von Auskunfteien auf die Erhebung des Auskunftsentgeltes (§ 34 Abs. 3 BDSG) verzichten. Im übrigen werden für die Auskunft an den Betroffenen im allgemeinen Beträge zwischen DM 10 und DM 25 verlangt. Die Aufsichtsbehörden haben in Fällen, in denen das Auskunftsentgelt erheblich über dem Satz der Datenschutzgebührenordnung lag, von den Unternehmen eine detaillierte Kostenaufstellung verlangt. Dies führte im Regelfall zur Reduzierung der Entgeltforderung.

Ein weiteres Beispiel für Vereinbarungen mit der Wirtschaft ist die Regelung mit der Schufa, wonach die Übermittlungsempfänger den Betroffenen auf die eingeholte Schufa-Auskunft hinweisen, wenn aufgrund negativer Angaben Kreditanträge abgelehnt werden. Diese für den Datenschutz des Betroffenen wichtige Übereinkunft ist Bestandteil der vertraglichen Vereinbarungen zwischen der Schufa und ihren Anschlußpartnern. Eine entsprechende gesetzliche Regelung hatte der Initiativentwurf der CDU/CSU-Fraktion vorgesehen (vgl. 3. TB S. 10; auch Nr. 6.2 dieses Berichts).

Durch diese Vereinbarungen wurden einige wesentliche Verbesserungen erreicht. Allerdings haben sich nicht alle Unternehmen der Branche den Vereinbarungen unterworfen. Die Vereinbarungen sind außerdem jederzeit aufkündbar. Schließlich kann ihre Einhaltung mit den Mitteln der Aufsicht nicht durchgesetzt werden. Die getroffenen Vereinbarungen ändern somit nichts an der Notwendigkeit einer gesetzlichen Regelung. Für die gegenwärtige Lage ist es kennzeichnend, daß sich einige Unternehmen zielstrebig einer datenschutzmäßigen Überprüfung entziehen konnten.

Die kritische Einstellung der Bürger zur Datenverarbeitung durch Auskunfteien beruht wesentlich auf zwei Mängeln, den immer wieder auftretenden Personenverwechselungen und der ungenügenden Aufklärung der Betroffenen.

Personenverwechselungen ziehen für den Betroffenen mitunter erhebliche materielle und immaterielle Folgen nach sich: z. B. Ruf- und Bonitätsschädigung, geplatzte Finanzierungen, Scheitern von Vertragsverhandlungen und aufwendige Bemühungen, falsche Angaben zu widerlegen. Zu Personenverwechselungen kommt es, wenn die Auskunftei nicht mit der erforderlichen Sorgfalt vorgeht und z. B. sich mit zu wenigen übereinstimmenden Merkmalen begnügt oder bei nur teilweise übereinstimmenden Angaben von der Personengleichheit ausgeht und es versäumt, den Empfänger der Auskunft auf die Ungewißheit der Angaben mit der gebotenen Deutlichkeit hinzuweisen.

Ich halte es nicht für vertretbar, mit dem Hinweis auf das Massengeschäft (allein ca. 20 Mio. Auskünfte durch die Schufa) bei der Datenverarbeitung großzügiger zu verfahren oder darauf zu vertrauen, daß Unstimmigkeiten beim Empfänger der Auskunft schon aufgedeckt würden. Die Verantwortlichkeit für negative Folgen aufgrund mangelnder Sorgfalt liegt eindeutig bei den Auskunfteien.

Auch heute noch sehen viele Bürger in der Tätigkeit der Auskunfteien eine Verletzung des Datenschutzes. Dem sollte durch bessere Aufklärung begegnet werden. Dabei sollte auch zum Ausdruck kommen, wie der Datenschutz gewährleistet wird und insbesondere wie der Betroffene seine Auskunfts- und Korrekturansprüche wahrnehmen kann.

4.3 Wohnungsvermietung

4.3.1 Mieterfragebögen

In meinem Vierten Tätigkeitsbericht (S. 45) hatte ich über die zunehmende Praxis von Vermietern berichtet, Mietinteressenten die Beantwortung von Fragebögen über ihre persönlichen und wirtschaftlichen Verhältnisse abzuverlangen. Problematisch ist die Vorgehensweise deshalb, weil die Fragen zum Teil erheblich in die Privatsphäre der Betroffenen eingreifen (z. B. „Sind Sie schwerbehindert? Wenn ja, Prozent-Satz!"; „Vorstrafen"; „Verwandtschaftsverhältnis sonstiger Haushaltsangehöriger"; „Haben Sie einen Teilzahlungskredit in Anspruch genommen?"; „Sind die in die Wohnung einzubringenden Sachen Ihr freies und unbelastetes Eigentum?"; Bescheinigung des bisherigen Vermieters, daß es sich bei dem Betroffenen um einen ordentlichen Mieter und pünktlichen Mietzahler handelt).

Der für das Mietrecht zuständige Bundesminister der Justiz hat mir im Einvernehmen mit dem Bundesminister für Raumordnung, Bauwesen und Städtebau Mitte 1982 mitgeteilt, an einer Reihe von Fragen sei ein legitimes Interesse des Vermieters nicht zu erkennen; er halte solche Fragen für eine mißbräuchliche Ausnutzung der schwierigen Lage von Wohnungsuchenden. Dennoch erscheine es ihm problematisch, mit gesetzgeberischen Maßnahmen gegen solche Praktiken vorzugehen. Ausgangspunkt der rechtlichen Beurteilung sei der Grundsatz, daß der Vermieter frei sei in der Entscheidung, mit wem er einen Mietvertrag abschließen will. Um

diese Entscheidung sinnvoll zu treffen, müsse er sich über die für das Mietverhältnis bedeutsamen Umstände unterrichten können. Dieses Informationsinteresse des Vermieters sei je nach Lage des Einzelfalles stärker oder weniger stark ausgeprägt. Die Formulierung einer gesetzlichen Regelung müsse notwendigerweise allgemein sein, könne also die schwierige Abgrenzung zwischen zulässigen und unzulässigen Fragen kaum zufriedenstellend lösen.

Der Bundesminister der Justiz erwartet, daß durch die Rechtsprechung anhand von Einzelfällen die Grenzen des Zumutbaren und Zulässigen herausgearbeitet werden. Er verweist auch auf die in der Literatur vertretene Auffassung, daß sich die arbeitsrechtliche Rechtsprechung zum Fragerecht des Arbeitgebers auf die entsprechende mietrechtliche Problematik übertragen lasse. Bei dieser Sachlage erscheine ihm jedenfalls zur Zeit ein Eingreifen des Gesetzgebers nicht angezeigt. Er werde jedoch die tatsächliche und rechtliche Entwicklung in diesem Bereich aufmerksam verfolgen.

Ich begrüße es, daß die zuständigen Ministerien meine Einschätzung des Problems teilen und daß man die weitere Entwicklung mit Aufmerksamkeit verfolgen will. Das Warten auf einschlägige Rechtsprechung bedeutet aber, daß für längere Zeit soziale Ungerechtigkeiten und Verletzungen des Persönlichkeitsrechts in Kauf genommen werden.

Auf einem wenn auch kleinen Sektor des gesamten Wohnungsmarktes könnten — so meine ich — Bund und Länder mit gutem Beispiel vorangehen. Soweit Mietobjekte mit öffentlichen Mitteln gefördert werden, könnte der öffentliche Geldgeber in die Bedingungen für die Subventionsvergabe einen Passus aufnehmen, der sich mit dem Fragerecht des künftigen Vermieters beschäftigt. Die Behörden könnten sich Mieter-Fragebögen vorlegen lassen, zu weitgehenden Informationswünschen entgegentreten und im äußersten Fall bei Zuwiderhandlungen die Kündigung des Subventionsvertrages androhen.

Dieses Vorgehen könnte ein erster Schritt sein, die Praxis zu beinflussen und Maßstäbe für die Begrenzung der Informationsanforderungen von Vermietern zu entwickeln. Ich möchte alle in Frage kommenden Stellen bitten, diesen Vorschlag aufzugreifen und den Datenschutzaufsichtsinstanzen über Erfahrungen zu berichten.

4.3.2 Heizkostenabrechnung

Die Arbeitsgemeinschaft der Verbraucher, die u. a. auch über Möglichkeiten des Energiesparens berät, hat mir Beschwerden im Zusammenhang mit der Heizkostenabrechnung vorgetragen. Mietern, die zur Kontrolle ihrer Abrechnung die Verbrauchswerte der übrigen Mietparteien erfahren wollen, wurde dies von Vermietern unter Hinweis auf den Datenschutz verwehrt.

Ich habe zu dieser — hauptsächlich im privaten Bereich auftretenden — Problematik Stellung genommen, weil auch die Bundesvermögensverwaltung als Vermieter zahlreicher Wohnungen auftritt.

Nach meiner Beurteilung liegt in der Bekanntgabe aller Verbrauchswerte im allgemeinen keine Beeinträchtigung schutzwürdiger Belange. Ausgangspunkt meiner Überlegungen war die seit März 1981 geltende Verordnung über die verbrauchsabhängige Abrechnung der Heiz- und Warmwasserkosten (BGBl. I S. 261 ff.). In der Verordnung wird für zentral beheizte Wohnungen geregelt, daß die Heizkosten zum einen Teil nach einem pauschalen Schlüssel (z. B. der Wohnungsgröße) und zum anderen Teil nach dem erfaßten individuellen Verbrauch verteilt werden.

Um die Richtigkeit der Abrechnung einer Mietpartei nachvollziehen und überprüfen zu können, ist es notwendig, sowohl alle Rechnungen und Kostenbelege als auch die Verteilung dieser Kosten auf die Mietparteien offenzulegen. Zwangsläufig werden dadurch Angaben über die Wohnungsgröße jeder einzelnen Mietpartei sowie den Heizverbrauch pro Wohnung (nicht jedoch pro Wohnraum) bekannt.

Die Offenlegung einer solchen Abrechnung ist — falls die Angaben dateimäßig verarbeitet werden und keine spezielle Rechtsvorschrift für die Bekanntgabe vorliegt — anhand der Übermittlungsregeln des § 24 BDSG zu beurteilen.

Nach der ersten Alternative ist die Weitergabe von Daten zulässig, wenn sie im Rahmen des Vertragsverhältnisses liegt. Den Rahmen des Vertragsverhältnisses bilden die zwischen den Parteien bestehenden vertraglichen Vereinbarungen, Absprachen und sonstigen Regelungen sowie die bei einem Mietverhältnis überlicherweise bestehenden gegenseitigen Rechte und Pflichten. Da der Vermieter zu einer verbrauchsabhängigen Heizkostenabrechnung und zu einer kontrollierbaren Gesamtabrechnung gesetzlich verpflichtet ist, ist eine Aufgliederung nach Wohnparteien nicht zu vermeiden. Eine dataillierte Abrechnung liegt daher m. E. im Rahmen der Abwicklung des Vertragsverhältnisses.

Die Bekanntgabe kann auch auf die zweite Alternative des § 24 BDSG gestützt werden. Danach ist eine Abwägung zwischen den berechtigten Interessen eines jeden Mieters an einer detaillierten Abrechnung und den schutzwürdigen Belangen der jeweiligen anderen Mieter vorzunehmen. Das berechtigte Interesse an einer solchen Kostenaufstellung kann man m. E. bejahen. Schutzwürdige Belange dürften in aller Regel nicht verletzt werden, da die Angaben einerseits wenig sensibel sind und andererseits jeder Betroffene in Bezug auf die eigenen Kontrollmöglichkeiten auch Vorteile aus dem Verfahren ziehen kann.

5 Datensicherung

Es ist eine allgemeine Erfahrung, daß Vorschriften über Sicherheitsmaßnahmen oft wenig ernst genommen werden und das Sicherheitsbewußtsein in vielen Bereichen ziemlich gering ist. So erregen z. B. Meldungen, daß bei einer Untersuchung sicherheitstechnischer Einrichtungen an 4 000 Baustellen über 7 000 Mängel festgestellt wurden, kaum besonderes Aufsehen, und Pflichten z. B. zum Tragen von Schutzhelmen oder zum Anlegen von Sicherheitsgurten werden nur lückenhaft erfüllt.

Bezogen auf die Sicherung von Daten sind die Verhältnisse nur wenig anders, zumindest wenn man den Sicherungsbedarf betrachtet, der über die Sicherung der Funktionsfähigkeit der Datenverarbeitung hinausgeht.

Sicherungsmaßnahmen bedeuten reale und ständige Belastungen, denen lediglich mögliche und seltene Schadensereignisse gegenüberstehen. Beim Datenschutz wirkt sich zusätzlich aus, daß die Art der Gefährdung selbst nicht so konkret erfahrbar ist wie etwa beim Unfallschutz. Soweit überhaupt Fälle von unbefugtem Zugang zu Daten oder unbefugten Eingriffen in die Datenverarbeitung bekannt werden, handelt es sich meist um Angriffe auf das Vermögen oder die Leistungsfähigkeit der datenverarbeitenden Stelle. Nur ganz selten stehen personenbezogene Daten im Mittelpunkt, etwa wenn Daten über Beschäftigte an Versicherungsunternehmen gelangen. Doch dabei ist das Ziel nicht die Beeinträchtigung schutzwürdiger Belange der Betroffenen, sondern die Anbahnung von Verträgen. So ist es verständlich, daß die Motivation für Datensicherungsmaßnahmen gelegentlich nur gering ist. Andererseits hat jeder Bürger, der einer Behörde seine personenbezogenen Daten anvertraut oder von dem eine Behörde ohne seinen Willen Daten speichert, einen Anspruch darauf, daß die Behörde mit diesen Daten sorgfältig umgeht und auch Vorkehrungen gegen unbefugte Verarbeitung oder Kenntnisnahme trifft. Es ist also durchaus sinnvoll, die Vorschrift des § 6 BDSG, nach der technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes zu treffen sind, so auszulegen, daß stets angemessener Schutz gegen unbefugtes Handeln vorzusehen ist. Als Minimum gilt es, wenigstens Möglichkeiten zu schaffen, um unbefugtes Handeln nachträglich zu entdecken.

Wenn die Art der verarbeiteten Daten oder die vermuteten Gefährdungen es nahelegen, muß der Schutz so verstärkt werden, daß er unbefugtes Handeln erschwert und die Entdeckung sehr wahrscheinlich ist.

Als Ergebnis meiner Kontroll- und Beratungstätigkeit kann ich feststellen, daß sich diese Ansicht zunehmend durchsetzt, auch wenn die Vorkehrungen gelegentlich noch unzureichend sind.

5.1 Die Bedeutung der Dateien-Übersicht

In § 15 BDSG ist vorgeschrieben, daß eine Übersicht über die Art der gespeicherten personenbezogenen Daten, über die damit zu erfüllenden Aufgaben und über die Empfänger der Daten geführt wird. Ich habe mich wiederholt dafür eingesetzt, daß diese Übersicht als eine möglichst vollständige und alle Aspekte umfassende Beschreibung der Datenverarbeitung einer Stelle angelegt wird und daß sie insbesondere alle Lagerstellen von Daten und die Transportvorgänge nachweist oder zumindest erkennen läßt. Der Aufwand für die dazu erforderliche Bestandsaufnahme und die Fortschreibung mag im Einzelfall hoch sein, diese Maßnahme ist aber stets angemessen. Denn ohne die Kenntnis der tatsächlichen Verhältnisse kann man weder die Datenverarbeitung insgesamt verantworten noch beurteilen, ob die bereits getroffenen Sicherungsmaßnahmen unter den jeweils gegebenen Verhältnissen auch ausreichend sind.

Zu Beginn meiner Beratungs- und Kontrolltätigkeit entsprachen die bei den geprüften Behörden geführten Übersichten diesen Anforderungen nur in Ausnahmefällen. Inzwischen hat sich aber die Erkenntnis weitgehend durchgesetzt, daß der Datenschutz in einer Behörde nur gewährleistet werden kann, wenn den dafür Verantwortlichen bekannt ist, auf welche Weise die Datenverarbeitung im einzelnen erfolgt. In einigen Fällen, so z. B. bei der Bundesanstalt für Arbeit und beim Deutschlandfunk, konnte ich durch meine Beratung auch für umfangreiche Probleme eine sachgerechte Lösung unterstützen.

5.2 Technische Mittel zur Datensicherung

Schon in meinem Ersten Tätigkeitsbericht (S. 66) hatte ich darauf hingewiesen, daß viele Anwender von ADV-Verfahren einige Sicherungsmaßnahmen deshalb nicht treffen können, weil die Betriebssysteme der ADV-Anlagen dies nicht genügend unterstützen. Inzwischen sind auf diesem Gebiet und auch in anderen Bereichen von den Herstellern verstärkte Bemühungen unternommen worden. Damit stehen für den Anwender im allgemeinen ausreichende Ansätze für Sicherungsmaßnahmen zur Verfügung, deren Nutzung aber für bereits laufende Anwendungen zum Teil erheblichen Aufwand erfordert.

Einige der angebotenen Sicherungsmöglichkeiten sind außerdem nur in Software-Paketen enthalten, die zusätzlich gekauft oder gemietet werden müssen, was deren Einsatz hemmt.

In Gesprächen mit Herstellern von Datenverarbeitungsanlagen habe ich mich über die Entwicklung informiert und mich bemüht, mit den Erfahrungen

aus meiner Tätigkeit Hinweise auf noch offene Probleme zu geben. Diesen Zielen dienten auch Veranstaltungen, die von den Datenschutz-Kontrollinstanzen mit verschiedenen Herstellern durchgeführt wurden. Dabei hat sich gezeigt, daß die Hersteller durchaus bereit sind, Forderungen nach mehr Sicherheit aufzugreifen und in Angebote umzusetzen. Das Ziel ihrer Bemühungen ist zwar in erster Linie die Sicherheit der Verfügbarkeit und der Schutz der Vermögenswerte des Anwenders, davon profitiert aber auch der Datenschutz. Diese Aktivitäten der Hersteller stoßen bei den Anwendern jedoch auf wenig Gegenliebe, denn die zusätzlichen Aufwendungen und die Furcht, eine vermeintlich erforderliche große Flexibilität zu verlieren, wirken oft stärker als das nur schwach ausgeprägte Sicherheitsbedürfnis.

Daß trotz dieser Schwierigkeiten die Sicherheit der Datenverarbeitung zunehmend an Interesse gewinnt, beweisen viele Beispiele:

— Seit langem ist die Idee eines TÜV-Siegels für datenschutzgerechte oder allgemeiner für sichere Hard- und Software im Gespräch. Bedenkt man den Entwicklungs- und Testaufwand, der für DV-Anlagen und Betriebssysteme zu leisten ist, und die Schwierigkeiten, fehlerfreie Systeme zu erstellen, so wird klar, daß dieses umfassende Ziel in absehbarer Zeit kaum erreichbar ist. Als einen Einstieg in diese Problematik bearbeitet der TÜV-Bayern zur Zeit ein Forschungsprojekt „Prüfung kommerziell angebotener Mehrbenutzer-Betriebssysteme von Minirechnern nach Gesichtspunkten der Datensicherung“. Die enge, deshalb aber auch realistische Zielsetzung dieses vom Bundesminister für Forschung und Technologie geförderten Projekts verspricht einen Erfolg, der besonders den Anwendern kleinerer Systeme helfen wird. Im Beirat zu diesem Forschungsprojekt wirkt ein Vertreter meiner Dienststelle mit.

— Die Datenfernübertragung auf Leitungen und Funkstrecken ist nicht abhörsicher und könnte mit geeigneten Geräten auch automatisch analysiert werden. Die wirksame Gegenmaßnahme „kryptographische Veschlüsselung“ ist aber erst dann im großen Umfang einsetzbar, wenn die Verfahren einheitlich festgelegt sind. An der entsprechenden Normungsarbeit wirkt ein Vertreter meiner Dienststelle mit.

  Die Bundesversicherungsanstalt für Angestellte plant wegen der durch die besondere geographische Lage bedingten Dringlichkeit unabhängig vom Fortschritt der Normung für ihre Datenfernübertragung von und nach Berlin (West) im Jahr 1983 die Verschlüsselung einzusetzen.

— Beim Transport von Datenträgern ist der Mehraufwand an Porto, aber auch an Organisation, besonders spürbar. Da eventuelle Verluste durch andere Sicherungsmaßnahmen ausgeglichen werden können, ist dieser Mehraufwand ausschließlich durch den Datenschutz verursacht und wird oft besonders kritisch bewertet. So möchte eine Krankenkasse für die Zusendung des von einem Dienstleistungsunternehmen mikroverfilmten Migliederverzeichnisses keine Sicherungsmaßnahmen treffen, weil bisher keine Unregelmäßigkeiten bekannt geworden sind. Es setzt sich aber zunehmend durch, daß für größere Mengen personenbezogener Daten, wie z. B. im Datenträgeraustausch für Aufgaben der Sozialversicherung, besondere Versandarten (Wertbrief, Wertpaket) gewählt werden.

— Die Protokollierung aller Verarbeitungsschritte, die eine Datenverarbeitungsanlage durchführt, liefert einen wertvollen Ansatzpunkt zur nachträglichen Kontrolle, ob jede durchgeführte Verarbeitung durch einen entsprechenden Arbeitsauftrag der zuständigen Fachabteilung veranlaßt war. In der Regel genügen eine grobe Durchsicht der Protokolle und gelegentlich stattfindende exakte Stichprobenkontrollen als angemessene Maßnahmen. Dies wird von verschiedenen Stellen so praktiziert, es gibt aber auch noch Stellen, bei denen diese Form der Kontrolle noch unzureichend ausgebaut ist.

— Bei der Vernichtung von Unterlagen mit zu schützenden Daten war es durch Mangel an Sorgfalt zu einigen Pannen gekommen. Bei meinen Kontrollen konnte ich feststellen, daß die Bundesbehörden auch diesen Teil der Datenverarbeitung ernst nehmen. Außerdem hat das Angebot an sicheren Vernichtungsmöglichkeiten zugenommen, und ein Unterausschuß des Fachausschusses Büromaschinen des Deutschen Instituts für Normung, in dem auch ein Vertreter meiner Dienststelle mitarbeitet, hat einen Normungsvorschlag für entsprechende Anlagen erarbeitet, um den Anwendern künftig die Auswahl zu erleichtern.

— Zugangskontrollen zu Rechenzentren, aber auch zu anderen Räumen zur Aufbewahrung oder Verarbeitung von Daten werden zunehmend eingeführt. Dies ist auch eine Folge der allgemeinen Bedrohung öffentlicher Einrichtungen sowie der Tendenz zur Arbeitszeiterfassung. Da die Zugangskontrollsysteme ständig verbessert werden, wird ihr Einsatz flexibler und trägt zur Unterstützung dieser Sicherungsmaßnahmen bei.

— Die Datenträgerverwaltung wird verstärkt durch automatisierte Systeme unterstützt. Aber auch dort, wo sich dies nicht lohnt, setzen sich Verfahren durch, die es ermöglichen, jederzeit festzustellen, wo sich ein Datenträger bzw. ein Datenbestand planmäßig befinden müßte. Noch selten werden jedoch stichprobenmäßige Inventuren (Soll-Ist-Vergleich) durchgeführt.

5.3 Die ordnungsgemäße Anwendung der DV-Programme

Die in § 15 Satz 2 Nr. 2 BDSG geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, leidet noch immer unter mangelhafter Dokumentation der ein-

gesetzten Verfahren. Dies liegt daran, daß die Entwicklung und der Einsatz von Entwurfs-, Programmier- und Dokumentationstechniken der großen Komplexität vieler Verfahren nicht gerecht wurden und daß deshalb häufig ausreichende Vorschriften für die Verfahrensentwicklung und -dokumentation nicht vorlagen oder nicht eingehalten wurden. Allein aus Gründen des Datenschutzes kann man eine Änderung dieses Zustandes, die erhebliche Eingriffe in die Organisation erfordert, jedoch nur in extremen Fällen erreichen.

Inzwischen ist die Entwicklung von Entwurfs-, Programmier- und Dokumentationstechniken vorangeschritten und es hat sich gezeigt, daß der wirtschaftliche Einsatz von DV-Verfahren auf Dauer erschwert wird, wenn die Verfahrensentwicklung nicht sinnvoll strukturiert und die erstellten Programme nicht übersichtlich dokumentiert sind. Dies hat zur Folge, daß bei der Entwicklung neuer und bei tiefgreifenden Änderungen alter Verfahren häufiger die nötige Transparenz und damit auch die Kontrollierbarkeit geschaffen werden, was auch dem Datenschutz entgegenkommt.

5.4 Dezentralisierung der Datenverarbeitung

Das Angebot an kleinen, leistungsfähigen und relativ billigen Datenverarbeitungsanlagen nimmt ständig zu. Damit ist es möglich, Datenverarbeitungsleistungen unterschiedlicher Art dezentral in den Verwaltungen einzusetzen, und zwar nicht nur so, daß über Terminals eine zentrale Anlage dezentral genutzt wird, sondern auch so, daß ein wesentlicher Teil der Verarbeitung unabhängig von der Zentrale erfolgt. Beispiele dafür sind die Schalterterminals bei den Fahrkartenausgaben, aber auch neuere Datenerfassungsgeräte und Textverarbeitungssysteme, die wegen ihres Funktionsreichtums auch für Datenverarbeitung genutzt werden können. Außerdem werden zunehmend Kleincomputer für begrenzte Aufgaben genutzt.

Aus der Sicht des Datenschutzes liegen die Vorteile dieser Entwicklung in der Überschaubarkeit der Abläufe und im Wegfallen von lediglich aus technischen Gründen notwendigen Datentransporten. Selbst wenn solche Anlagen in größere Systeme eingebettet sind, bleibt als Vorteil, daß nur die sachlich erforderlichen Datenweitergaben erfolgen und die Schnittstellen eindeutig festgelegt sein müssen.

Für die Sicherung der Daten gegen unbefugte Nutzung ergeben sich jedoch neue Probleme, weil in kleinen Systemen, die oft nur von einer Person benutzt werden, eine Funktionentrennung oder das bewährte Vier-Augen-Prinzip nicht eingehalten werden können. Außerdem werden oft die Abläufe nicht protokolliert, und die verwendeten Datenträger (Kassetten, Disketten, Minidisketten) sind so klein und handlich, daß ihre Mitnahme unbemerkt bleiben würde. Die damit entstehenden Sicherungsprobleme werden zwar etwas entschärft, weil die vorkommenden Fallzahlen je Anlage meist nur niedrig sind, für sensible Bereiche, z. B. in der Arbeits- und Sozialverwaltung, könnte die gewünschte Dezentralisierung aber dadurch unzulässig werden, daß die erforderliche Sicherheit nicht gewährleistet werden kann.

6 Entwicklung des Datenschutzrechts

6.1 Allgemeines

In der „Chronik“ des Deutschen Bundestages für die 8. Wahlperiode 1976 bis 1980 (herausgegeben vom Presse- und Informationszentrum des Deutschen Bundestages), Seite 64, ist folgendes zu lesen:

> Auf der Suche nach einer Leitlinie für die den Bereich „Verwaltung“ betreffende Parlamentstätigkeit wird man auf keinen Grundsatz häufiger treffen als auf den der Konkretisierung und damit Verschärfung des Datenschutzrechts. Anlaß zu allgemeinen Aussprachen im Plenum und im Innenausschuß über die Entwicklung des Datenschutzes bieten die jährlichen Berichte des Bundesbeauftragten für den Datenschutz. Vorrangiges gesetzgeberisches Ziel ist die Ausfüllung und Präzisierung der Generalklauseln des Bundesdatenschutzgesetzes in sogenannten bereichsspezifischen Datenschutzbestimmungen. Über die Novellierungsbedürftigkeit auch des Bundesdatenschutzgesetzes besteht zwischen allen Fraktionen Einigkeit. Die Beratungen der eingebrachten Gesetzentwürfe konnten jedoch nicht mehr abgeschlossen werden.

Als Beispiele für bereichsspezifische Datenschutzregelungen nennt die „Chronik“ anschließend das Bundesstatistikgesetz, das Statistikbereinigungsgesetz, das Volkszählungsgesetz 1981 und das Melderechtsrahmengesetz. An den Vorbereitungen und an den parlamentarischen Beratungen dieser Gesetze habe ich mich gemäß meinem gesetzlichen Auftrag beteiligt. Ich bin immer wieder dafür eingetreten, das Datenschutzrecht vor allem bereichsspezifisch weiterzuentwickeln, weil das BDSG als Auffangsgesetz konzipiert ist und schon aus diesem Grundverständnis heraus nicht allen erst im konkreten Verwaltungsvollzug sichtbar werdenden Bedürfnissen und spezifischen Gefährdungen Rechnung tragen kann und soll. Daher habe ich es begrüßt, daß auf verschiedenen Gebieten — auch über die vorstehend genannten hinaus — dieses Anliegen aufgegriffen worden ist und vom Gesetzgeber nach Abwägung der Interessen der Betroffenen und der datenverarbeitenden Stellen die jeweils angemessenen konkreten Datenschutzregelungen geschaffen wurden. Im einzelnen wird auf sie an anderer Stelle dieses Berichts eingegangen. Die — wie ich hoffe — fortdauernden Bemühungen um eine bereichsspezifische Weiterentwicklung des Datenschutzrechts sollen jedoch nicht den Eindruck erwecken, als werde eine Überarbeitung des BDSG selbst dadurch entbehrlich.

6.2 Novellierung des BDSG

Die Novellierung des BDSG ist ein Thema, das seit Verabschiedung des Gesetzes in Fachkreisen und in einer interessierten Öffentlichkeit leidenschaftlich diskutiert wird. Auch ich habe mich in allen meinen bisherigen Tätigkeitsberichten dazu geäußert und Vorschläge unterbreitet. Die Diskussion begann bereits bei der Verabschiedung des Gesetzes, als im Parlament die baldige Novellierung des Gesetzes gefordert wurde, zu der man nur noch erste praktische Erfahrungen bei seiner Anwendung abwarten wollte. Der Verlauf der Diskussion wird markiert durch die Vorlage von Gesetzentwürfen der Bundestagsfraktionen im Januar/Februar 1980 und eines Gesetzentwurfs des Bundesministers des Innern im März 1982. Keiner der Entwürfe ist bisher Gesetz geworden — ein sicheres Zeichen für die Schwierigkeit der Problematik und die in vielerlei Hinsicht unterschiedlichen Interessenlagen der mit der Anwendung des Gesetzes Befaßten, insbesondere der Normadressaten, der Kontrollinstitutionen und der Betroffenen.

Über die bei Erlaß des Gesetzes noch nicht absehbaren Wirkungen der neuen Rechtsmaterie liegen inzwischen reichlich Erfahrungen vor. Ich habe sie in meinen bisherigen Tätigkeitsberichten geschildert; die zahlreich vorhandene Fachliteratur hat sich ihrer angenommen; langsam, aber in zunehmendem Maße hat sich auch Rechtsprechung zum Datenschutzrecht herausgebildet. Das Fazit ist — mit Einschränkungen — positiv. Anfängliche Kritik an den Generalklauseln des Gesetzes hat sich weitgehend als unbegründet erwiesen, was im wesentlichen darauf zurückzuführen ist, daß in manchen Bereichen, in denen sich Unsicherheit einstellte oder die Generalklauseln unangemessene Ergebnisse hervorbrachten, bereichsspezifische und auf das jeweilige Anwendungsgebiet zugeschnittene Datenschutzvorschriften erlassen wurden. Prognosen, die die Anwendung des Gesetzes durch angebliche Praxisferne und Bürgerunfreundlichkeit belastet sahen, wurden nicht selten auch dadurch widerlegt, daß datenschutzbewußte Anwender Auslegungen wählten, die den Schutz des Bürgers stärker betonten und ihm Vorrang vor anderen Interessen einräumten. Doch auch andere Interpretationen waren zu beobachten, wo die vom Gesetz eingeräumten Spielräume zugunsten der datenverarbeitenden Stelle, bequemer oder rationeller Aufgabenerfüllung ausgeschöpft wurden. Zuweilen ließen sich aber auch beide Positionen miteinander verbinden.

Ich habe in meinen Publikationen und öffentlichen Äußerungen wiederholt meinen Eindruck wiedergegeben, daß sich das BDSG im großen und ganzen in der Praxis bewährt hat, daß es aber gleichwohl einige erhebliche Mängel aufweist und insbesondere dort verbesserungsbedürftig ist, wo nur durch teleologische und keineswegs auch für die Zukunft gesicherte Rechtsauslegung angemessene Ergebnisse erzielt werden können. Beide Bewertungen

habe ich in einer dem BMI zugeleiteten umfangreichen Ausarbeitung, die unter dem Titel „Ziele und Mittel des Datenschutzes" veröffentlicht wurde (vgl. 4. TB S. 54), eingehend begründet. Die wichtigsten meiner darin vorgelegten Vorschläge zur Novellierung des BDSG habe ich in meinem Vierten Tätigkeitsbericht (S. 53 ff.) dargestellt. Eine Reihe dieser Vorschläge, die sich teilweise auch auf frühere Überlegungen anderer Stellen und auf die Initiativentwürfe der Bundestagsfraktionen der 8. Legislaturperiode stützen, sind im Referentenentwurf des BMI vom März 1982 aufgegriffen worden. Der Referentenentwurf, der einer Ankündigung in der Regierungserklärung vom 24. November 1980 folgte, bietet aktuellen Anlaß, sich mit dem Thema erneut zu befassen, zumal auch aus der neuen Bundesregierung verlautet, daß an der Absicht, das BDSG zu novellieren, festgehalten werde.

Meine Beurteilung des Referentenentwurfs ist in eine gemeinsame Stellungnahme des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz eingegangen, die ich dem BMI unter dem 25. Juni 1982 zugeleitet habe. Ich verzichte auf eine vollständige Wiederholung dieser Ausführungen und beschränke mich im folgenden auf die wichtigsten Punkte, wobei weitergehende Überlegungen aufgrund interner und öffentlicher Erörterungen bereits mitberücksichtigt werden.

Ich nenne an erster Stelle diejenigen Neuerungen, die ich inhaltlich und zum Teil auch in der vorgelegten Formulierung uneingeschränkt begrüße. Dazu gehören insbesondere die Einführung eines verschuldensunabhängigen Schadensersatzanspruchs bei unrichtiger oder unzulässiger Verarbeitung personenbezogener Daten; die Unentgeltlichkeit des Auskunftsrechts des Betroffenen; die Streichung der nach den bisherigen Erfahrungen wenig wirksamen Verpflichtung auf das Datengeheimnis und der Pflicht zur Veröffentlichung über die gespeicherten Daten (§ 12 BDSG), die mehr Aufwand als die erwartete Transparenz der Datenverarbeitung verursacht hat; ferner die ausdrückliche Zweckbindung übermittelter Daten beim privaten Empfänger; die primäre Löschungspflicht für nicht mehr erforderliche Daten anstelle der bisherigen Sperrung in diesen Fällen; im vierten Abschnitt die Verpflichtung des Empfängers übermittelter Daten, diese und die übermittelnde Stelle dem Betroffenen mitzuteilen, wenn aufgrund der Datenübermittlung eine „Negativentscheidung" getroffen wird. Als Fortschritt bewerte ich ferner die Stärkung der Stellung der Aufsichtsbehörden im nicht-öffentlichen Bereich, die nun befugt sein sollen, auch aus anderen Anlässen als einer konkreten Beschwerde eines Betroffenen tätig zu werden, schließlich auch die Erweiterung des bei meiner Dienststelle geführten Dateienregisters um diejenigen Dateien der Behörden und öffentlichen Stellen des Bundes, die nicht automatisiert betrieben werden und bisher nur in den (künftig entfallenden) Veröffentlichungen nach § 12 BDSG verzeichnet waren; ich sehe darin eine Verbesserung meines Kontrollinstrumentariums und — infolge der mir auferlegten Verpflichtung zur übersichtlichen Veröffentlichung des so vervollständigten Registerinhalts — eine Möglichkeit, mehr Transparenz der Datenverarbeitung herzustellen.

Ich habe auch häufig darauf hingewiesen, daß ich Auflockerungen der Datenschutzvorschriften unterstütze, soweit dies vertretbar erscheint, insbesondere dann, wenn im Normalfall eine Beeinträchtigung des Betroffenen nicht zu befürchten oder nur geringfügig ist und von ihm durch eigenes Handeln ausgeschlossen werden kann. Dies gilt beispielsweise für die im BMI-Entwurf vorgesehene Zulassung der Übermittlung von Daten, die im Rahmen eines Vertragsverhältnisses gespeichert sind, für Zwecke der Werbung oder der Sozial- oder Marktforschung, verbunden mit einem Widerspruchsrecht der Betroffenen.

Andere Vorschriften des Referentenentwurfs sind nach meiner Auffassung weniger gelungen und bedürfen kritischer Überprüfung.

6.2.1 Datenerhebung

Ich bin seit jeher dafür eingetreten, die in § 9 Abs. 2 BDSG enthaltene Regelung der Datenerhebung zu verbessern, weil es sich dabei um einen Vorgang handelt, der Voraussetzung für alle weiteren, vom Gesetzgeber für schutzwürdig befundenen Datenverarbeitungsschritte ist, diese in Gang setzt und den ersten und damit entscheidenden Eingriff in die Persönlichkeitssphäre des Betroffenen darstellt. Die Zulässigkeit der Datenerhebung wird von § 9 Abs. 2 BDSG vorausgesetzt, indem dort davon ausgegangen wird, daß die Datenerhebung entweder durch eine Rechtsvorschrift außerhalb des BDSG legitimiert ist oder der Betroffene seine Daten freiwillig hergibt. Das Gesetz verpflichtet die datenerhebende Stelle lediglich, den Betroffenen auf die Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hinzuweisen.

Ich habe zu dieser Vorschrift stets die Auffassung vertreten, daß sie unabhängig davon gilt, ob die erhobenen Daten später in Dateien gespeichert werden oder nicht (vgl. 2. TB S. 61; 3. TB S. 11). Für meine Auffassung spricht, daß der von § 1 Abs. 2 Satz 1 BDSG geforderte Dateibezug nur für die geschützten Phasen der Datenverarbeitung gilt — die Datenerhebung gehört nicht dazu — und nicht immer von vornherein feststeht, ob eine Speicherung der erhobenen Daten in einer Datei erfolgen wird. Diese Auslegung ist umstritten. Mein Anliegen ging deshalb dahin, eine Klarstellung in meinem Sinne herbeizuführen und ferner die Aufklärungspflicht auszubauen.

Offenbar anknüpfend an den Initiativentwurf der CDU/CSU, Drucksache 8/3608, sieht der Referentenentwurf des BMI statt dessen vor, die Datenerhebung als weitere Phase der Datenverarbeitung in das Regelungswerk des BDSG einzubeziehen. Diese Lösung erscheint mir nach erneutem Überdenken nicht akzeptabel, weil sie zu der aus den vorgenannten Gründen abzulehnenden Beschränkung auf Daten führt, die in Dateien gespeichert werden sollen. Der BMI-Entwurf sieht diese Beschränkung an anderer Stelle (§ 1 Abs. 2 Satz 1) auch ausdrücklich

vor. Ferner wird die Zulässigkeit der Datenerhebung an die gleichen Voraussetzungen gebunden, wie sie für die Datenspeicherung gelten. Damit geht die Regelung ins Leere, weil der Schutz gegen eine zu weitgehende Erhebung bereits durch die Zulässigkeitsbeschränkungen der Datenspeicherung gewährleistet ist. Andererseits besteht die Gefahr, daß die vorgesehene Generalklausel als zusätzliche Erhebungsermächtigung aufgefaßt wird, die in ihrer weit gefaßten Formulierung problematisch wäre.

Den Interessen der Betroffenen wäre durch bessere Aufklärung mehr gedient, die sich auch darauf erstrecken sollte, ob die der Datenerhebung zugrundeliegende Rechtsvorschrift eine Verpflichtung zur Angabe von Daten enthält, welcher weiteren Verwendung die Daten zugeführt werden sollen und welche Folgen eine Verweigerung von Angaben hat. Darüber hinaus wiederhole ich meine frühere Forderung, im Gesetz klarzustellen, daß die Aufklärungspflicht unabhängig davon besteht, ob die Daten in eine Datei eingehen, und daß durch die Art und Weise der Datenerhebung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden dürfen.

6.2.2 Interne Dateien

Ich begrüße es, daß der BMI-Entwurf den Anwendungsbereich des BDSG hinsichtlich interner, d. h. nicht zur Übermittlung an Dritte bestimmter und außerhalb automatisierter Verfahren verarbeiteter Daten präzisiert. Diese Daten sollen künftig auch dem Datengeheimnis unterliegen. Sie müssen in die nach den §§ 15, 29 und 38 BDSG zu führende Übersicht aufgenommen werden. Letzteres ist auf erheblichen Widerstand bei den datenverarbeitenden Stellen gestoßen, was mich dazu veranlaßt, nachdrücklich auf die Notwendigkeit einer solchen Regelung hinzuweisen, die übrigens weitgehend der Praxis — jedenfalls bei den von mir geprüften Bundesbehörden — entspricht. Die Übersicht dient der internen Transparenz, sie bildet den Einstieg für die Datenschutzkontrolle und ermöglicht es der datenverarbeitenden Stelle, für die ihr gesetzlich obliegende Sicherstellung des Datenschutzes zu sorgen. Wären interne Dateien in der Übersicht nicht enthalten, könnte weder die datenverarbeitende Stelle noch die Kontrollinstanz feststellen, ob es sich tatsächlich um interne Dateien handelt und ob die wenigen für diese geltenden BDSG-Vorschriften eingehalten sind. Im übrigen umfaßt meine Kontrollbefugnis in bestimmten Beziehungen auch interne Dateien, obwohl weder im geltenden Recht noch im BMI-Entwurf § 19 BDSG unter den auf interne Daten anwendbaren Vorschriften genannt ist. In der Praxis haben sich daraus keine Probleme ergeben, doch scheint es mir im Interesse der Rechtsklarheit wünschenswert, dies auch im Gesetz zu verdeutlichen.

6.2.3 Medienprivileg

Die von mir für notwendig erachtete Einschränkung des Medienprivilegs (4. TB S. 57) durch Gewährung von Rechten auf Gegendarstellung, Auskunft und Berichtigung ist im BMI-Entwurf nunmehr vorgesehen — allerdings in nach meinem Dafürhalten noch unzureichender Form. Die neuen Regelungen, die aus Kompetenzgründen lediglich die Rundfunkanstalten des Bundesrechts verpflichten, räumen dem Betroffenen ein Auskunfts- und Berichtigungsrecht erst nach erfolgter Berichterstattung ein. Ich habe Zweifel, ob diese Einschränkung bei richtiger Abwägung der gleichrangigen Grundrechte der Artikel 2 und 5 GG verfassungsrechtlich tatsächlich geboten ist. Ich verkenne die große Bedeutung der Pressefreiheit nicht, doch höre ich immer wieder von Fällen, in denen durch unrichtige oder ungenaue Berichterstattung in den Medien schutzwürdige Belange der Betroffenen nachhaltig beeinträchtigt werden, und es stößt oft auf Unverständnis, daß den Betroffenen keine rechtlichen Mittel zur Verfügung stehen, dies schon vorbeugend zu verhindern, zumal die nachträgliche Berichtigung und die Gegendarstellung meist wirkungslos bleiben.

6.2.4 Einwilligung

Hinsichtlich der Einwilligung sieht der BMI-Entwurf zwar eine Verpflichtung der datenverarbeitenden Stelle vor, den Betroffenen über die Bedeutung der Einwilligung in geeigneter Weise aufzuklären, doch fehlen Vorgaben über den Mindestinhalt dieser Unterrichtung. Ich verweise hierzu auf meine früheren Forderungen (4. TB S. 55). Neuere Überlegungen zielen darauf ab, die Aufklärung nur noch für den Fall vorzuschreiben, daß der Betroffene sie ausdrücklich verlangt. Ich hielte dies für eine wenig bürgerfreundliche Lösung. Wenn die Einwilligung schriftlich, meist durch Vordruck, erbeten wird, bedeutet es kaum nennenswerten Mehraufwand, eine einmal formulierte Belehrung beizufügen, anstatt den Betroffenen zu zwingen, Rückfragen zu stellen und weiteren Schriftwechsel zu führen. Insbesondere bei Verweigerung der Einwilligung wird sich der Betroffene über die Folgen häufig nicht im klaren sein und auch nicht danach fragen. Eine vorausgehende Aufklärung gerade zu dieser Entscheidungsmöglichkeit scheint mir besonders wichtig und regelungsbedürftig.

6.2.5 Datenverarbeitung für Zwecke der wissenschaftlichen Forschung

Der von Datenschutzbeauftragten wie von Wissenschaftlern gleichermaßen mit Nachdruck erhobenen Forderung nach einer Spezialvorschrift für die Datenverarbeitung zu Forschungszwecken kommt der BMI-Entwurf nach. Ich habe in meinem Vierten Tätigkeitsbericht (S. 57) inhaltliche Vorstellungen für eine solche Regelung entwickelt. Sie sind im BMI-Entwurf ebenso wie in weiteren Bemühungen um eine verbesserte Fassung nur zum Teil berücksichtigt. Ich fasse sie deshalb hier nochmals thesenartig zusammen:

— Die Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung bedarf grundsätzlich der Einwilligung der Betroffenen und ist nur für ein bestimmtes For-

schungsvorhaben zulässig. Dies sollte in einer Regelung deutlich hervorgehoben werden.

— Ist die Einholung der Einwilligung unzumutbar, so ist zu prüfen, ob unter Berücksichtigung des Forschungszwecks Grund zur Annahme besteht, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden. Das hiermit gemeinte Erfordernis einer Abwägung zwischen den beiderseitigen Interessen sollte in einer Gesetzesformulierung eindeutig zum Ausdruck kommen.

— Ungeachtet dessen muß gelten, daß die Verarbeitung personenbezogener Daten unzulässig ist, wenn sich der Forschungszweck auch auf andere Weise erreichen läßt. Ist dies nicht der Fall, so muß sichergestellt sein, daß die Daten anonymisiert werden, sobald der Forschungszweck es erlaubt.

— Werden personenbezogene Daten an einen Forschungsträger übermittelt, so hat die übermittelnde Stelle die Art der übermittelten Daten, den Empfänger und den Forschungszweck aufzuzeichnen, um die Kontrollierbarkeit zu gewährleisten und den Vorgang transparent zu machen.

— Es ist ein „Forschungsgeheimnis" zu statuieren, das sicherstellt, daß die zu Forschungszwecken gespeicherten oder übermittelten Daten ohne Einwilligung des Betroffenen nicht weiter übermittelt und nicht für andere als Forschungszwecke verwendet werden. Insoweit sollten keine Auskunfts- und Zeugnispflichten bestehen sowie keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien oder Datenträgern. Eine Bestimmung dieser Art fehlt im BMI-Entwurf.

Die anhaltende, mit großen Engagement, mitunter sogar mit unnötiger Schärfe geführte Diskussion über das Thema „Datenschutz und wissenschaftliche Forschung" (s. oben Nr. 2.8) veranlaßt mich, auf eine angemessene, den beiderseitigen Interessen hinreichend gerechtwerdende und vor allem baldige gesetzliche Lösung zu drängen, damit der Konfliktstoff dauerhaft beseitigt wird.

6.2.6 Datenübermittlung

Zur Datenübermittlung bringt der Entwurf wichtige Neuerungen. Verbunden mit einer Änderung der Legaldefinition für die Übermittlung, wie ich sie in meinem Vierten Tätigkeitsbericht (S. 56) gefordert habe, wird versucht, eine Regelung für die bisher umstrittenen Zulässigkeitsvoraussetzungen von Direktzugriffsverfahren zu finden. Nachdem der Entwurf eine kaum praktikable Lösung vorsah, weil dort auf die strikte Erforderlichkeit des Verfahrens abgestellt wurde, ist nunmehr in der weiteren Diskussion eine Fassung entstanden, die im Kern meinen Vorstellungen Rechnung trägt: Die zum Abruf bereitgehaltenen Daten müssen ihrer Art nach für den Empfänger erforderlich sein und das Direktzugriffsverfahren muß unter Berücksichtigung der Belange aller Beteiligten, insbesondere auch der Betroffenen, angemessen sein. Die zur Durchführung des Verfahrens vorgeschriebenen Festlegungen der Einzelheiten sollen den beteiligten Stellen überlassen bleiben; ich würde eine Entscheidung der jeweils obersten Dienstbehörden bevorzugen. In meinem Vierten Tätigkeitsbericht (a. a. O.) habe ich vorgeschlagen, wegen des Gefährdungsrisikos von Online-Anschlüssen eine Unterrichtung des Bundesbeauftragten vorzuschreiben. Dieser Anregung soll offenbar nicht gefolgt werden, ebenso nicht meiner Forderung, die Einrichtung von automatisierten Direktzugriffsverfahren zwischen Sicherheitsbehörden unter den Vorbehalt einer besonderen Rechtsvorschrift zu stellen. Insbesondere die letztere Forderung wiederhole ich an dieser Stelle, weil es sich m. E. hier um einen zusätzlichen Eingriff in die Rechte der Betroffenen handelt, der einer speziellen Rechtsgrundlage bedarf.

Eine andere Vorschrift soll die Verantwortung für die Zulässigkeit von Datenübermittlungen festlegen. In den Erörterungen zum BMI-Entwurf wurde — zu Recht — gerügt, daß sich dabei Widersprüche zu den Amtshilfevorschriften im Verwaltungsverfahrensgesetz, im Sozialgesetzbuch X und in der Abgabenordnung ergeben. In schlage demgegenüber vor, nicht die Verantwortung zu verteilen, sondern zu bestimmen, wem die *Prüfung* der einzelnen Zulässigkeitskriterien obliegt. Insbesondere halte ich es nicht für vertretbar, für den Fall, daß die Übermittlung zur rechtmäßigen Erfüllung der Aufgaben des Empfängers, also in dessen Interesse erfolgt, diesem die alleinige Verantwortung für die Zulässigkeit zu übertragen. Ich habe vielmehr — in der gemeinsamen Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder — angeregt, die Zulässigkeitsprüfung auch im vorgenannten Fall primär der übermittelnden Stelle aufzuerlegen, und zwar im allgemeinen beschränkt auf die Frage, ob das Ersuchen des Empfängers im Rahmen seiner Aufgaben und Befugnisse liegt und — wenn im Einzelfall hierzu Anlaß besteht — auch hinsichtlich Erforderlichkeit der Übermittlung und Rechtmäßigkeit der Aufgabenerfüllung.

Die Verlagerung der Prüfung im Einzelfall auf die Stelle, die diese Daten anfordert, könnte zu einer unkontrollierten Selbstbedienung führen, wenn die abrufende Stelle insoweit weder einer Kontrolle unterworfen noch überhaupt zur Einhaltung der Vorschriften des BDSG angehalten wird. Dies würde immer dann gelten, wenn die abrufende Stelle die abgerufenen Daten nicht in einer eigenen Datei verarbeitet und der Abruf auch nicht Folge einer solchen Verarbeitung ist. Die Regelungen über die Zulässigkeit von Übermittlungen müssen deshalb auch denjenigen Empfänger binden, der eine Übermittlung auslöst, und die Kontrollkompetenz der jeweils für den Empfänger zuständigen Instanz muß sich auch auf diese Vorgänge erstrecken.

6.2.7 Auskunftsrecht

Einem in der Vergangenheit vielfach geäußerten Grundanliegen entspricht der BMI-Entwurf, indem er die Kostenfreiheit des Auskunftsanspruchs des

Betroffenen festlegt. Der vereinzelt dagegen vorgebrachte Einwand, daß damit Mißbräuchen Tür und Tor geöffnet werde, läßt sich mit dem Hinweis auf allgemeine Rechtsgrundsätze zur Abwehr mißbräuchlicher Rechtsausübung und auf die im Gesetz vorgesehene Möglichkeit der Auskunftsverweigerung bei Gefährdung der Aufgabenerfüllung bzw. der Geschäftszwecke und Ziele der speichernden Stelle entkräften. Eine begrüßenswerte Erweiterung des Auskunftsrechts ist auch insofern vorgesehen, als — im öffentlichen wie im nicht-öffentlichen Bereich — das Auskunftsrecht nunmehr auch auf Herkunft und Empfänger der Daten erstreckt wird. Die ebenfalls neue Regelung des Auskunftsverweigerungsrechts befriedigt indessen noch nicht. Das Auskunftsverweigerungsrecht der Polizei, der Bundesanwaltschaft und der Finanzbehörden ist nunmehr in Anlehnung an die KpS- und Dateien-Richtlinien insofern eingeschränkt worden, als es ausdrücklich von dem Ergebnis einer Abwägung der schutzwürdigen Belange des Betroffenen mit dem öffentlichen Interesse an der Nichtherausgabe der Daten abhängig gemacht wird. Dies ist ein Fortschritt. Allerdings ist nicht einsehbar, weshalb die gleiche Regelung nicht auch für das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und den Militärischen Abschirmdienst sowie andere sicherheitsrelevante Behörden des Bundesministers der Verteidigung eingeführt wird, für die keine Auskunftspflicht besteht. Die Geheimhaltungsinteressen dieser Behörden ließen sich auch bei einer Gleichstellung durchaus wahren, sie wären — was ich für sachgerecht halte — lediglich zu einer Einzelfallprüfung verpflichtet (vgl. oben Nr. 3.2.4).

Eine nach meiner Auffassung notwendige Klarstellung fehlt leider im BMI-Entwurf. Die Finanzbehörden berufen sich auf ihr Auskunftsverweigerungsrecht bei allen Aufgaben, die sie im Anwendungsbereich der Abgabenordnung erfüllen. Das BDSG fügt dieser Privilegierung jedoch die Einschränkung hinzu, daß es sich um Aufgaben „zur Überwachung und Prüfung" handeln muß (s. oben Nr. 2.3.2). Wenn die dazu vertretene Auffassung des Bundesministers der Finanzen richtig wäre, daß alle Aufgaben im Anwendungsbereich der Abgabenordnung ausnahmslos der Überwachung und Prüfung dienen, hätte es dieses einschränkenden Zusatzes nicht bedurft. Die Novellierung des BDSG bietet Gelegenheit, diese Zweifelsfrage zu klären.

6.2.8 Stellung des Bundesbeauftragten für den Datenschutz

Die als Ziel des Novellierungsentwurfs u. a. genannte Stärkung der Stellung des BfD erschöpft sich darin, daß dem BfD über den geplanten Aufbau personenbezogener automatisierter Informationssysteme Nachricht zu geben und ferner die Auswahl, Versetzung und Abordnung seiner Mitarbeiter von seinem Einvernehmen abhängig zu machen ist. Letztere begrüßenswerte Festlegung entspricht einer seit Bestehen des Amtes mit dem Bundesminister des Innern vereinbarten Praxis, die auf die Unabhängigkeit des Bundesbeauftragten Rücksicht nimmt.

Die Unterrichtungspflicht über geplante Informationssysteme, die aus dem Initiativentwurf der SPD/FDP (Drucksache 8/3703) stammt, ist nur dann geeignet, meine Kontrolltätigkeit zu unterstützen, wenn sie über die bloße Mitteilung der Tatsache einer Planung hinausgeht und auch inhaltliche Aussagen über die geplante Maßnahme enthält. Sofern zur Erläuterung der Vorschrift eine Definition des Begriffs „Informationssystem" in die Begründung aufgenommen wird, wäre darauf zu achten, daß keine zu enge Beschreibung gewählt wird. Den planenden Stellen sollte daran gelegen sein, schon frühzeitig meine Beratung, die stets auch Erfahrungen mit anderen und möglicherweise vergleichbaren Systemen einbezieht, in Anspruch nehmen zu können.

Wichtige Ergänzungen des Gesetzes, die ich — mehr zur Klarstellung meiner Position — wiederholt gefordert und von einer Novellierung auch erwartet habe, fehlen indessen im Entwurf. Ich halte es für dringlich, den in meinen bisherigen Tätigkeitsberichten mehrfach behandelten Meinungsstreit über den Umfang meiner Kontrollkompetenz gesetzlich zu entscheiden. Es geht dabei um die Frage, ob meine Kontrollbefugnis hinsichtlich der Einhaltung „anderer Vorschriften über den Datenschutz" i. S. d. § 19 Abs. 1 Satz 1 BDSG auch die Einhaltung solcher Datenschutzvorschriften einschließt, die die Datenverarbeitung ohne Beschränkung auf Dateien regeln. Meine Argumente für eine extensive Auslegung dieser Vorschrift habe ich ausführlich in meinem Dritten Tätigkeitsbericht Seite 57 f. (vgl. auch 4. TB S. 54 und 57 und oben Nr. 1.3.3) dargestellt und verzichte hier auf eine Wiederholung. Ich gehe davon aus, daß der Gesetzgeber sich ihnen nicht verschließen wird, wenn er sich die Stärkung der Stellung des Bundesbeauftragten zum Ziel gesetzt hat.

Zu den anderen Vorschriften über den Datenschutz gehören gemäß § 45 Satz 2 Nr. 1 BDSG auch § 30 AO (Steuergeheimnis) und § 5 Postgesetz (Post- und Fernmeldegeheimnis). Es ist widersinnig, daß dem Bundesbeauftragten, der die Wahrung dieser Geheimnisse zu kontrollieren hat, eben diese bei seiner Kontrolle entgegengehalten werden. Zumindest hinsichtlich des Steuergeheimnisses muß deshalb § 19 BDSG als gesetzliche Ausnahmevorschrift angesehen werden, während eine Ausnahme vom Post- und Fernmeldegeheimnis gemäß Artikel 19 Abs. 1 Satz 2 GG einer ausdrücklichen, das einschränkende Grundrecht des Artikel 10 GG bezeichnenden Vorschrift bedarf. Auch dieses Anliegen ist aus meinen Tätigkeitsberichten (vgl. 4 TB S. 57) bekannt, wurde aber gleichwohl im BMI-Entwurf nicht aufgegriffen.

Zur Stärkung der Stellung des Bundesbeauftragten könnte auch eine Vorschrift beitragen, die dem Bundesbeauftragten und seinen Mitarbeitern ein Zeugnisverweigerungsrecht einräumt. Abgesehen von ihrer Signalwirkung nach außen würde eine solche Vorschrift denjenigen der Datenschutzkontrolle unterliegenden Behörden entgegenkommen, die besondere Geheimhaltungsinteressen haben.

6.2.9 Datenverarbeitung im nicht-öffentlichen Bereich

Bei der Würdigung der Änderungsvorschläge des BMI-Entwurfs zu den Vorschriften über die Datenverarbeitung im nicht-öffentlichen Bereich kann ich zwar nicht auf unmittelbar selbst gesammelte Erfahrungen zurückgreifen, weil dieser Bereich nicht zu meiner Kontrollzuständigkeit gehört. Aus meiner Kooperation mit den Aufsichtsbehörden der Länder (§ 19 Abs. 5 BDSG) und aus Eingaben, die fälschlicherweise an mich gerichtet werden, gewinne ich jedoch Erkenntnisse zu diesem Bereich, deren Verwertung im Rahmen der BDSG-Novellierung mir nützlich erscheint.

Der BMI-Entwurf versucht die Praktikabilität der sogenannten listenmäßigen Datenübermittlung (§ 24 Abs. 3 BDSG) zu verbessern, indem er die erleichterte Übermittlung von listenmäßig zusammengefaßten Daten einer Personengruppe nicht nur auf die im Gesetz aufgeführten (Grund-)Daten, sondern zusätzlich auch auf die (beliebige) Angabe über die Zugehörigkeit der Betroffenen zu der Personengruppe erstreckt. Da es sich dabei um höchst sensible Angaben handeln kann, sollte hier zumindest eine Eingrenzung vorgenommen werden. Aber auch damit bleibt die listenmäßige Datenübermittlung problematisch, weil sie die Übermittlung von Daten einer Personenmehrheit erleichtert, während die Übermittlung der gleichen Datenarten für nur einen Betroffenen den strengeren Zulässigkeitsvoraussetzungen des § 24 Abs. 1 unterliegt.

Erfreulich ist, daß dem betrieblichen Datenschutzbeauftragten nunmehr ein besonderer Kündigungsschutz gewährt werden soll. Die vorgeschlagene Lösung, den Kündigungsschutz für Betriebsratsmitglieder entsprechend anzuwenden, geht jedoch fehl. Denn der Kündigungsschutz würde entfallen, sobald der Datenschutzbeauftragte von seinem Amt abberufen wird. Zu bevorzugen wäre deshalb eine Regelung, die die Bestellung und Abberufung des Beauftragten an die Zustimmung des Betriebsrates bindet und — als flankierende Maßnahme — die Kündigung des Arbeitsverhältnisses nur aus wichtigem Grund zuläßt.

Ich vermisse im BMI-Entwurf eine nicht nur von mir vorgeschlagene (vgl. 4. TB S. 57) Regelung, die für Daten des Arbeitsverhältnisses eine stärkere Zweckbindung als für sonstige im Rahmen von Vertragsverhältnissen gespeicherte Daten vorschreibt. Insbesondere sollte der Übermittlungsgrund des berechtigten Interesses eines Dritten entfallen. Auch der Einwilligung des Betroffenen sollte bei der Verarbeitung von Arbeitnehmerdaten nur begrenzte Rechtswirkung beigemessen werden, weil die Entscheidungsfreiheit des Betroffenen hier faktisch eingeschränkt ist.

So sehr die sachgerechte Erweiterung der Befugnisse der Aufsichtsbehörden im nicht-öffentlichen Bereich (§ 30 BDSG) zu begrüßen ist, um so bedenklicher erscheint es, daß privatrechtliche Einrichtungen der öffentlich-rechtlichen Religionsgesellschaften der staatlichen Datenschutzkontrolle gänzlich entzogen werden sollen, zumal es sich hier häufig um reine Wirtschaftsbetriebe handelt. Gewisse Einschränkungen bei der Kontrolle dürften ausreichen, um dem verfassungsrechtlichen Status dieser Einrichtungen gerecht zu werden.

In meinem Vierten Tätigkeitsbericht (S. 58) hatte ich angeregt, dem Betroffenen mit der Benachrichtigung über die erstmalige Speicherung seiner Daten (§ 24 Abs. 1 BDSG) auch mitzuteilen, welcher Art die gespeicherten Daten sind und an wen sie voraussichtlich regelmäßig übermittelt werden sollen. Dies würde letztlich aufwandsmindernd wirken, weil es viele der sonst nachfolgenden Auskunftsersuchen entbehrlich machte. Leider hat der BMI-Entwurf diesen Vorschlag, den ich hiermit wiederhole, nicht übernommen.

6.2.10 Strafvorschrift

Für die weitere Vorbereitung des Referentenentwurfs weise ich aufgrund meiner Erfahrungen auf eine Lücke in der Strafvorschrift des § 41 BDSG hin. Bisher nicht erfaßt sind dort die Tatbestände des Erschleichens von Daten durch unrichtige Angaben mit der Folge, daß eine unzulässige Datenübermittlung ausgelöst wird, ferner die unbefugte Wiederherstellung des Personenbezugs für anonymisierte Daten — ein Gesetzesverstoß, der insbesondere im Rahmen der Datenverarbeitung zu Zwecken wissenschaftlicher Forschung künftig zunehmend Relevanz gewinnen kann. Ein Strafantragsrecht des Bundesbeauftragten, das nur im Einvernehmen mit dem Betroffenen ausgeübt werden kann, würde dessen strafrechtlichen Schutz abrunden.

Ich hoffe, daß die Novellierung des BDSG, deren Notwendigkeit alle Fraktionen des Deutschen Bundestages durch Vorlage eigener Entwürfe in der 8. Legislaturperiode sichtbar anerkannt haben, zügig weiterbetrieben wird und bald zum Abschluß gebracht werden kann.

7 Datenschutz im Ausland, internationale Zusammenarbeit

7.1 Die Datenschutzgesetzgebung im internationalen Vergleich

Rein äußerlich betrachtet hat sich der Stand der Datenschutzgesetzgebung im Ausland seit dem Ersten Tätigkeitsbericht nur unwesentlich verändert. Verfügten Ende 1978 acht westliche Länder über ein mehr oder weniger umfassendes nationales Datenschutzgesetz (neben der Bundesrepublik: Dänemark, Frankreich, Kanada, Neuseeland, Norwegen, Österreich, Schweden), so sind in der Zwischenzeit nur drei kleinere Länder hinzugekommen (Luxemburg, Israel und Island). Tatsächlich hat sich die Situation jedoch grundlegend gewandelt. Konnte man seinerzeit noch zweifeln, ob sich das Konzept eines umfassenden, durch gesetzlich verbürgte Rechte des einzelnen und unabhängige Kontrolle gekennzeichneten Datenschutzes allgemein durchsetzen würde, so steht dies spätestens seit der Unterzeichnung der Datenschutzkonvention des Europarates am 28. Januar 1981 jedenfalls für die Mitgliedsländer des Europarats eindeutig fest. Die Philosophie dieser Konvention, in den einzelnen Ländern einen bestimmten Mindest-Datenschutz zu sichern und im gleichen Zuge auszuschließen, daß der grenzüberschreitende Datenverkehr diskriminiert wird, stellt jedes Land, das die Gefahr datenschutzbedingter Wettbewerbsnachteile im internationalen Wirtschaftsverkehr vermeiden will, vor die Notwendigkeit, durch nationale Datenschutzgesetzgebung die in der Konvention enthaltenen Anforderungen zu erfüllen. Insofern ist es nicht überraschend, daß die Länder, die bisher noch zurückstehen, ihre Bemühungen sichtlich verstärkt haben. Die Erfahrungen derjenigen Länder, die schon seit längerem Datenschutzgesetze haben, werden verstärkt in Anspruch genommen. Der Europarat unterstützt den Erfahrungsaustausch durch gemeinsam mit interessierten Ländern veranstaltete Tagungen, im Jahre 1982 z. B. in Paris und Rom.

Zumindest für die westeuropäischen Länder läßt sich heute feststellen, daß die Notwendigkeit gesetzlicher Vorkehrungen für den Datenschutz allgemein anerkannt wird; nur über die Ausgestaltung im einzelnen gehen — angesichts der unterschiedlichen Rechtssysteme kaum verwunderlich — die Vorstellungen noch auseinander.

Die Entwicklung im Ausland zu verfolgen, bedeutet, zugleich die Frage zu stellen, wo die Bundesrepublik Deutschland heute steht. Dabei muß man sich allerdings im klaren sein, daß es wegen der vielfältigen relevanten Aspekte sehr schwierig ist, zwei verschiedene Datenschutzsysteme nach ihrer Effektivität für den Schutz des Bürgers bewertend zu vergleichen. Dennoch kann man heute feststellen, daß der deutsche Gesetzgeber, als er Mitte der siebziger Jahre das Bundesdatenschutzgesetz konzipierte und dabei nur auf die begrenzten Erfahrungen des Landes Hessen und Schwedens zurückgreifen konnte, in den zentralen Fragen eine glückliche Hand hatte.

a) Das in Schweden entwickelte, vom deutschen Gesetzgeber verworfene Lizenzierungssystem hat zwar einige Nachahmer gefunden, wurde jedoch im Ursprungsland selbst schrittweise zurückgenommen und gilt dort heute nur noch für bestimmte Ausnahmefälle. Wo immer es flächendeckend angewendet wird oder wurde, hat es die Arbeitskraft der Kontrollinstitutionen stark absorbiert. Da diese aber überall nur über sehr wenig Personal verfügen, bedeutet jede Belastung mit Routinearbeit eine schwerwiegende Behinderung der Aufgabe, die wichtigsten inhaltlichen Probleme zu identifizieren, zu untersuchen und einer Lösung näherzubringen — ein Effekt, der vielleicht den zu kontrollierenden Instanzen nicht unangenehm, der Effektivität und dem Ansehen des Datenschutz aber höchst abträglich ist. Ein Kenner der internationalen Szene hat daher kürzlich vom „De-facto-Bankrott des Lizenzierungssystems" gesprochen.

b) Auch was die Frage der Einbeziehung von Daten juristischer Personen betrifft, gibt die Entwicklung im Ausland keinen Anlaß, die Lösung des BDSG in Zweifel zu ziehen. Es sind keine Fälle bekanntgeworden, in denen die Nicht-Anwendung der (allgemeinen) Datenschutzvorschriften zu einer Rechtslage geführt hat, die man als nicht tragbare Lücke im Rechtsschutz ansehen könnte.

c) Bestätigt hat sich auch die Richtigkeit der Einbeziehung der manuellen Datensammlungen. Von großer Bedeutung ist, daß das französische Datenschutzgesetz — entgegen dem ursprünglichen Entwurf — insoweit dem deutschen Vorbild entspricht. In denjenigen Ländern, in deren Gesetzen nur die automatisierte Datenverarbeitung geregelt ist, stellt sich immer wieder das Problem der Gesetzesumgehung; zudem wird es von den Bürgern als willkürlich empfunden, wenn ihnen die Auskunft verweigert oder die Weitergabe ihrer Daten an andere Stellen für unbedenklich erklärt wird, nur weil der betreffende Datenbestand nicht automatisiert geführt wird.

d) Auch die Lösung, spezielle Datenschutzvorschriften den Regelungen des Bundesdatenschutzgesetzes vorgehen zu lassen und auch bezüglich ihrer Einhaltung dem Bundesbeauftragten die Kontrolle zu übertragen, hat sich bewährt. In Ländern ohne entsprechende Regelung, wie etwa in Frankreich, ist den Datenschutzkontrollinstanzen in solchen Fällen wiederholt die Kompetenz bestritten worden. Nicht nur in der Bundesrepublik handelt es sich bei

Bereichen mit eigenen (und auch älteren) Datenschutzvorschriften oft und gerade um besonders sensible Bereiche.

7.2 Inter- und supranationale Datenschutzbestrebungen

Auf der internationalen Ebene war die Unterzeichnung der Datenschutz-Konvention des Europarates am 28. Januar 1981 das herausragende Ereignis der letzten Jahre. Die Konvention konnte jedoch bisher nicht in Kraft treten, da es dazu nach Artikel 22 der Ratifikation durch mindestens fünf Mitgliedstaaten bedarf. Bisher haben dreizehn Staaten das Übereinkommen unterzeichnet und damit ihre Beitrittsabsicht bekundet. Zur Ratifikation ist es lediglich in Schweden gekommen; in Frankreich, Dänemark und Norwegen steht sie kurz bevor. Naturgemäß wird von Ländern, die schon bisher im Datenschutz eine Führungsrolle einnahmen, erwartet, daß sie auch die Rafitikation des Übereinkommens nicht zögerlich betreiben. Deshalb ist es wünschenswert, daß die Bundesregierung in absehbarer Zeit den Entwurf eines Ratifikationsgesetzes vorlegt.

Der Europarat hat seine Aktivitäten auf dem Gebiet des Datenschutzes mit der Erarbeitung der Konvention nicht beendet, sondern bemüht sich nun um die Vereinheitlichung auch des bereichsspezifischen Datenschutzes.

a) Im Hinblick auf die Bestimmung der Datenschutz-Konvention, die bei der Datenverarbeitung zu Zwecken der Statistik oder der wissenschaftlichen Forschung bestimmte Ausnahmen von der Beachtung der Datenschutzgrundsätze zuläßt (Artikel 9 Abs. 3), wurden Richtlinien formuliert, die auf diesem Gebiet einen ausgewogenen Kompromiß zwischen den wissenschaftlichen Informationsbedürfnissen und dem Schutz der Betroffenen sicherstellen sollen. Der Richtlinientext liegt den Organen des Europarats zur Beschlußfassung vor.

b) Bereits weit gediehen sind auch die Empfehlungen zum Bereich Direktmarketing/Adressenhandel. Sie zielen insbesondere auf eine korrekte Information der Betroffenen über den sie betreffenden Datenfluß ab und stimmen insofern mit meinen Vorstellungen zur Novellierung des BDSG überein (vgl. 1. TB S. 49f). Mit der Verabschiedung wird im ersten Halbjahr 1983 gerechnet.

c) Mit den spezifischen Anforderungen an den Datenschutz im Bereich der sozialen Sicherung beschäftigt sich eine Arbeitsgruppe des Expertenkomitees in der Absicht, auch für dieses Gebiet besondere Empfehlungen zu entwickeln.

Darüber hinaus dient der Europarat weiterhin dem Austausch von Erfahrungen sowohl mit den generellen Datenschutzvorschriften als auch mit Spezialproblemen etwa im Zusammenhang mit Reisedokumenten oder zentralen Registern.

Die Haltung der Europäischen Gemeinschaften zum Datenschutz ist, wie schon in den vergangenen Jahren, abwartend. Kommission und Rat sehen keinen aktuellen Bedarf für den Erlaß einer EG-Richtlinie. Vielmehr sollen das Inkrafttreten der Europarats-Konvention und deren praktische Konsequenzen in den Ländern abgewartet werden.

Das Europäische Parlament hat — gestützt auf Vorschläge seines Rechtsausschusses (vgl. 4. TB S. 62) — am 9. März 1982 eine Entschließung zum Datenschutz verabschiedet (abgedruckt in Europäische Grundrechte-Zeitung 1982, S. 139). Auch die Überlegungen des Europäischen Parlaments orientieren sich vor allem an der Konvention des Europarats. Es bringt jedoch deutlich den Wunsch zum Ausdruck, daß die Organe der Europäischen Gemeinschaften wie auch die Mitgliedsländer selbst eine aktive Datenschutzpolitik verfolgen mögen. So werden die Mitgliedstaaten aufgefordert, die Konvention unverzüglich zu unterzeichnen, soweit dies noch nicht geschehen ist, und sie bis Ende des Jahres 1982 zu ratifizieren. Zu gegebener Zeit soll auch die Europäische Gemeinschaft der Konvention beitreten. Das Europäische Parlament hat die Kommission aufgefordert, eine Empfehlung an die Mitgliedstaaten zu richten, „um zu gewährleisten, daß die nationale Gesetzgebung zur Durchführung des Übereinkommens entsprechende Wirkung hat". In Anbetracht der schnellen technologischen Entwicklung hält das Parlament „eine regelmäßige Überprüfung der Anwendung von Datenverarbeitung und Übertragungstechniken auf Gemeinschaftsebene (für) erforderlich". Wenn sich die Datenschutz-Konvention des Europarats als unzureichend erweise, solle der Erlaß einer Gemeinschaftsrichtlinie erwogen werden. Dabei sei dann insbesondere dafür Sorge zu tragen, daß der Schutz sich auf alle Angaben persönlicher Art auch über die Grenzen hinweg erstreckt, daß er im privaten und im öffentlichen Bereich gleich ist, daß die Betroffenen ein Recht auf Zugang zu ihren Daten sowie auf deren Berichtigung haben, daß ein Schadensersatzanspruch besteht und daß der Betrieb von Datenbanken einer nationalen Anmelde- und Genehmigungspflicht unterliegt (zu dem letztgenannten Punkt vgl. aus meiner Sicht oben 7.1 a).

7.3 Zusammenarbeit der Datenschutzinstanzen

Mit den Problemen des Datenschutzes sieht sich jedes Land konfrontiert, dessen Wirtschaft und Verwaltung sich der modernen Informationstechnik bedienen. Datenschutz ist ein Problem der Informationsgesellschaft. Die nationalen Rechtsordnungen und Besonderheiten der jeweiligen Wirtschafts- und Sozialordnung mögen im Detail unterschiedliche Sichtweisen und unterschiedliche Ansätze der Problemlösung bedingen; die zentralen Themen — Machtzuwachs durch Nutzung der Informationstechnik, schwindende Transparanz des Geschehens in Großorganisationen und dem Individuum drohender Orientierungsverlust — stellen sich fast überall gleich. Veränderte Formen der Informationsverarbeitung, etwa bei den Sicherheitsbehörden oder bei der wissenschaftlichen Forschung, oder die Auseinandersetzung mit den absehbaren

Auswirkungen der Neuen Medien auf die Informationslandschaft sind gemeinsame Erfahrungen und Probleme zahlreicher Länder.

Internationaler Erfahrungsaustausch — für diejenigen, die technische Systeme entwickeln, seit jeher selbstverständlich — ist daher auch für die Einrichtungen, die mit der Datenschutzkontrolle betraut sind, unverzichtbar. Es ist deshalb erfreulich, daß sich die internationale Zusammenarbeit zwischen den Datenschutz-Kontrollinstitutionen binnen weniger Jahre fest etabliert hat und von den Beteiligten als Selbstverständlichkeit betrachtet wird. Im Anschluß an die 1. Internationale Konferenz der Datenschutz-Kontrollinstitutionen, zu der ich im Jahre 1979 nach Bonn eingeladen hatte, haben weitere Treffen in Ottawa, Paris und London stattgefunden. Ich halte es für gut, daß sich die Konferenz sowohl mit dem aktuellen Tagesgeschäft — etwa mit der Prüfung internationaler Informationssysteme der Polizei (vgl. oben Nr. 3.3.9), der Fluggesellschaften und der Banken — als auch mit den Grundfragen des Datenschutzes befaßt. Zu nennen sind hier beispielsweise die Probleme der zentralen Einwohnerregistrierung, des nationalen Personenkennzeichens und ähnlicher Nummernsysteme oder des Verhältnisses zwischen Datenschutz und Meinungs- und Pressefreiheit.

8 Ausblick

Das geltende Datenschutzrecht deckt bei weitem nicht alle regelungsbedürftigen Fragen der Informationsbeziehungen in Verwaltung, Wirtschaft und Gesellschaft ab — und dies wird und soll so bleiben. Der Normbereich des Datenschutzrechts ist allerdings wesentlich weiter als die dateimäßige Verarbeitung personenbezogener Daten, wie sie im BDSG und den Landesdatenschutzgesetzen geregelt ist; die „anderen Vorschriften über den Datenschutz" behandeln zahlreiche weitere Formen von Informationserhebung, -sammlung und -auswertung und bestimmen in sachnaher Vorgehensweise, welche Offenbarungen zulässig sind (s. a. oben Nr. 1.3.3 und 6.2.8). Dem entsprechen die Erwartungen vieler Bürger: durch Zuschriften und in Diskussionen erfahre ich immer wieder, daß der Datenschutzgedanke auf zahllose Informationsverhältnisse bezogen wird — auch auf solche, die z. B. durch besondere Geheimhaltungsgebote geprägt sind — und daß es als äußerst unbefriedigend empfunden wird, wenn mangels Dateibezuges (bei Unanwendbarkeit von Spezialnormen) kein datenschutzrechtlicher Ansatz zur Verbesserung des Informationsverhaltens vorhanden ist — so insbesondere wenn personenbezogene Daten nur in Akten verarbeitet werden.

Selbstverständlich kann und soll der Gesetzgeber nicht alle nur denkbaren Arten von Informationsbeziehungen regeln; vor allem müssen die *sozialadäquaten* Formen menschlicher Kommunikation von Reglementierungen möglichst ganz frei bleiben. Aber andererseits müssen heute alle hergebrachten Verfahrensweisen überdacht werden, und wenn bestimmte Praktiken sozial mächtiger Institutionen, insbesondere großer Verwaltungen, Unternehmen und Verbände immer wieder in Frage gestellt werden, kann dies ein Anzeichen für einen Bedarf an (Neu-)Regelung sein. Zumindest die Überprüfung traditioneller Erhebungs- und Mitteilungsweisen kann selbst bei der Justiz mit ihren starken rechtsstaatlichen Bindungen angebracht sein (s. a. oben Nr. 2.2.2).

Viele datenschutzrechtliche Maßgaben sind nicht nur für die unmittelbar Betroffenen bedeutsam, sondern für den weiteren Ausbau ganzer Informationssysteme. So haben die Erforderlichkeitsprüfungen, die nach §§ 9 Abs. 1 und 10 Abs. 1 Satz 1 BDSG angestellt werden, Auswirkungen auf die Zulässigkeit zentraler Datensammlungen. Ich erinnere an die Beschränkung des Kriminalaktennachweises auf Hinweise auf überregionale und schwere Straftaten (oben Nr. 3.3.5), an die Absage an eine Zentraldatei über medizinische Gutachten im Bereich der sozialen Sicherung in § 96 Abs. 3 SGB X und an den Vorschlag eines eigenen Ordnungsmerkmals im Arbeitsmedizinischen Dienst der Bau-Berufsgenossenschaften anstelle der Rentenversicherungsnummer (oben Nr. 2.15.3). Der Individualdatenschutz fungiert in solchen Fällen auch als „*Systemdatenschutz*" im Sinne von Adalbert Podlech: die Rechtsnormen, die zunächst „nur" individuelle Interessen schützen sollen, dienen dann auch dazu, das Allgemeininteresse an einer gerechten, überschaubaren und kontrollierbaren Ausgestaltung der Informationsbeziehungen zu sichern. Dadurch, daß das Individuum vor übermäßiger Überwachung geschützt wird, bleibt auch das Gemeinwesen „ausbalanciert". Man muß sich aber darüber im klaren sein, daß der Systemdatenschutz bisher noch nicht hinreichend konkret in Rechtsvorschriften ausgeprägt ist (Einzelheiten und weitere Beispiele bei Podlech, Individualdatenschutz-Systemdatenschutz, in: Beiträge zum Sozialrecht, Festgabe für H. Grüner, Percha am Starnberger See 1982, S. 451 f.).

Einige Landesdatenschutzgesetze enthalten ausdrückliche Vorschriften zur Stabilisierung eines Informationsgleichgewichts zwischen verschiedenen staatlichen/kommunalen „Gewalten". Das Urteil darüber, ob diese Bestimmungen sich bewährt haben, muß ich meinen Kollegen in den Ländern überlassen.

Verschiedene ausländische Datenschutzgesetze dienen auch dem Schutz von Daten über juristische Personen; diese Funktion wird in der Bundesrepublik teilweise von Spezialvorschriften des Handels- und Wirtschaftsrechts und von solchen Bestimmungen erfüllt, die Auskunftspflichten z. B. für statistische oder steuerliche Zwecke begründen — wie ich meine und wie die Erfahrungen der betreffenden anderen Länder belegen (s. o. 7.1 b), eine angemessene Lösung.

Manche meinen, Datenschutz stehe im Zielkonflikt zur Bürgerfreundlichkeit der Verwaltung. Ich teile diese Ansicht nicht. Ich halte es vielmehr für geboten, daß die Verwaltung sich datenschutzgerecht *und* bürgerfreundlich verhält, und in der Regel sind beide Ziele sehr wohl miteinander vereinbar (wie auch einige Beispiele in diesem Bericht belegen, etwa die erste Verordnung nach dem MRRG, die Neuregelung der Zivildienstüberwachung und die Ausführungen zur Formulargestaltung, s. o. 2.1.1, 2.1.4, 2.5.5, 2.11.1, 2.14.2, 2.15.6). Leistungsfähigkeit der Verwaltung und Eingehen auf die Interessen der Bürger widersprechen sich nur dann, wenn „Effizienz" mit Größe, Schnelligkeit und ähnlich formalen, vordergründigen Maßstäben gleichgesetzt wird.

Der Präsident des Bundesverfassungsgerichts, Ernst Benda, hat vor einiger Zeit vor der Tendenz zu immer größeren, immer perfekteren und unüberschaubaren Verwaltungseinheiten, Schulen, Krankenhäusern oder Gerichten gewarnt; sie berge die Gefahr in sich, daß der Bürger die innere Bezie-

hung zu seinem Gemeinwesen verliert (Frankfurter Rundschau vom 9. März 1982). In dieselbe Richtung — Gespräch statt Technik — weisen jüngst u. a. Äußerungen des bayerischen Innenministers Hillermeier zum Eindringen des Computers in die ärztliche Praxis (Süddeutsche Zeitung vom 30. 12. 1982). Dies sind Überlegungen, die bei der weiteren Arbeit am Informationsrecht beachtet werden sollten.

Es darf nicht sein, daß Datenschutzgründe zu unnötiger Informationsrationierung benutzt werden. Zwei Beispiele dafür, wie es nicht sein sollte: manche Gerichte löschen in Urteilsausfertigungen für Dritte nicht nur die Namen der Parteien/Angeklagten, sondern auch die der Richter — die doch eine amtliche Funktion erfüllen; ein Landgericht ließ aus einer Strafakte den Zentralregisterauszug des Beschuldigten entfernen, bevor es dem Verteidiger Einblick gewährte — das Bundesverfassungsgericht hob diese Entscheidung als „schlechterdings unhaltbar" auf. Weil ein großes Maß an Offenheit gegenüber dem Bürger zu den Bedingungen demokratischer Machtkontrolle gehört, befürworte ich auch die Einführung eines Informationszugangsrechts nach dem Vorbild der schwedischen und amerikanischen Gesetze über Aktenöffentlichkeit und „Freedom of Information" (selbstverständlich mit dem Vorbehalt der „privacy" des Betroffenen, also in sorgfältiger Abstimmung mit dem nötigen Datenschutz).

Auch wenn man den Datenschutz angemessen — weder zu eng noch zu weit — abgrenzt, ist er nicht für alle Probleme, die sich in den Informationsbeziehungen zwischen einzelnen untereinander und zu den politischen und gesellschaftlichen Organisationen stellen, das geeignete Regelungsprinzip. Die Entwicklung der Informationstechnik hat mehr und weiterreichende soziale Folgen als mit den Mitteln des Datenschutzrechts bewältigt werden können (es sei denn, man strapaziert den Datenschutzbegriff übermäßig). Man denke an die grundlegende Veränderung und den Abbau zahlloser Arbeitsplätze, aber auch an die ökonomischen und entwicklungspolitischen Fragen, die in letzter Zeit unter dem Titel „Weltinformationsordnung" diskutiert werden. Erst recht ist Datenschutz inadäquat, um etwa den Wettbewerb auf dem Markt für Computer, Datenfernübertragung und Informationsdienstleistungen zu lenken; die in den USA immer wieder aufgestellte Behauptung, das europäische Datenschutzrecht werde in diesem Sinne praktiziert, ist jedenfalls für die Bundesrepublik Deutschland abwegig. Weitere Problemkreise, die zu dem sich entwickelnden Recht der Informationsbeziehungen gehören, sind die Partizipation an der allgemeinen und Fachkommunikation (Stichwort: Fachinformationszentren), eine gerechte Entgeltregelung für Informationsurheber (besonders im Hinblick auf die Neuen Medien) und die kulturverfassungsrechtlichen Aspekte der neuen Informations- und Kommunikationsmedien (zu deren datenschutzrechtlichen Implikationen s. oben 2.6.2).

Dies alles kann hier nicht vertieft werden; ich habe mich zu verschiedenen Aspekten an anderer Stelle geäußert und werde die Diskussion über die gesellschaftlichen Auswirkungen der Informationstechnik auch künftig verfolgen. Denn „den Weg und die Schritte in die sogenannte Informationsgesellschaft dürfen wir nicht blind gehen" (Szyperski, Chancen und Risiken der Informationstechnologie, Schloßtag 1981 der Gesellschaft für Mathematik und Datenverarbeitung, in: Der GMD-Spiegel 4/1981 S. 66f.). Auch soweit Einschätzungen der Technologiefolgen keine unmittelbare Bedeutung für die datenschutzrechtliche Aussage haben, bilden sie — unvermeidlicherweise — wichtige Elemente des Verständnishintergrundes („Vorverständnis"), auf dem einzelne rechtliche Probleme zu sehen sind.

Ich hielte es jedenfalls für unangemessen, an der Durchsetzung datenschutzrechtlicher Rechtsnormen mitzuwirken, ohne über die sozialen Folgen der Datenverarbeitung und verwandter Technologien nachzudenken. Das heißt keineswegs, sozialwissenschaftliche Erkenntnisse unvermittelt in normative Aussagen umzusetzen; vielmehr müssen diese Erkenntnisse neben anderen Maximen bei der Rechtsetzung und bei der Nutzung vorhandener Spielräume in der Rechtsanwendung berücksichtigt werden. Die Auseinandersetzung um die richtige Verwirklichung des Datenschutzes darf also nicht allein von technischen und organisatorischen Wunschvorstellungen einerseits und rein rechtstechnisch-begrifflicher Argumentation andererseits bestimmt werden. Bei jeder Form von Rechtsverwirklichung ist es nötig, die voraussehbaren Folgen in die Abwägung einzubeziehen, erst recht bei der Durchsetzung einer angemessenen, menschlichen Ordnung der Informationsverarbeitung in einer von Technik und Organisation geprägten Welt. Die Aufgabe, eine solche Ordnung zu schaffen, ist schwer, aber sie ist lösbar.

Bonn, den 13. Januar 1983

Prof. Dr. H. P. Bull

Anhang

Bilanz zum Vorjahresbericht

In meinem Vierten Tätigkeitsbericht habe ich auf zahlreiche offengebliebene Fragen und Probleme hingewiesen. Wie die nachfolgende Aufstellung zeigt, konnten davon viele im Berichtsjahr gelöst werden, andere sind noch offen und in einigen Bereichen stehen sich nach wie vor gegensätzliche Rechtspositionen gegenüber.

(1) Zur Datenspeicherung beim Bundesamt für den Zivildienst (BAZ), insbesondere zur Speicherung der Religionszugehörigkeit, habe ich Bedenken geltend gemacht (4. TB S. 6 f.). Das BAZ speichert die Religionszugehörigkeit nur noch dann, wenn der Betroffene damit einverstanden ist; siehe dazu Nr. 2.1.4 in diesem Bericht.

(2) Damit Unterlagen aus der Gewissensprüfung der Kriegsdienstverweigerer nicht in den vom Bundesamt für den Zivildienst (BAZ) zu führenden Personalakten mitgeführt werden, hatte ich vorgeschlagen, diese Unterlagen bei dem Kreiswehrersatzamt zu belassen, bei dem die Prüfung durchgeführt wurde (4. TB S. 7). Diesem Vorschlag ist der Bundesminister für Verteidigung nicht gefolgt. Eine Lösung wurde dadurch gefunden, daß das BAZ diese Unterlagen getrennt von den sonstigen Akten und unter besonderem Verschluß aufbewahrt; siehe dazu Nr. 2.1.5 in diesem Bericht.

(3) Zur beabsichtigten Novellierung des Bundeszentralregistergesetzes hatte ich angeregt zu prüfen, ob die Eintragungen von Verfahrenseinstellungen wegen Schuldunfähigkeit und Eintragungen über aufgehobene Entmündigungen nicht schon vor dem Tode des Betroffenen gelöscht werden können (4. TB S. 42). Meine Vorschläge sind in den vorliegenden Entwürfen nicht berücksichtigt, ich habe sie deshalb dem Rechtsausschuß übermittelt; siehe dazu Nr. 2.2.1 in diesem Bericht.

(4) Für das Ausländerzentralregister und besonders für seine Mitbenutzung durch verschiedene Sicherheitsbehörden habe ich eine Neukonzeption und konkrete Entscheidungen des Gesetzgebers gefordert (4. TB S. 34). Der Bundesminister des Innern hält es für verfrüht, schon jetzt in gesetzgeberische Überlegungen zu diesem Thema einzutreten; siehe dazu Nr. 2.1.3 in diesem Bericht.

(5) Zur Anordnung über Mitteilungen in Zivilsachen habe ich Bedenken geäußert (4. TB S. 43). Die Diskussion zu einzelnen Problemkreisen ist vorangeschritten, eine geschlossene Empfehlung, die gemeinsam mit den Datenschutzbeauftragten der Länder erarbeitet werden soll, ist noch in Vorbereitung; siehe dazu Nr. 2.2.4 in diesem Bericht.

(6) Über Bemühungen, den Umfang der Mitteilungen in Strafsachen einzuschränken und für die verbleibenden Mitteilungen eine tragfähige Rechtsgrundlage zu schaffen, habe ich berichtet (4. TB S. 41). Der Bundesminister der Justiz teilte mit, daß die Justizminister des Bundes und der Länder eine bundesgesetzliche Regelung und eine Einschränkung des Umfangs der Mitteilungen für erforderlich halten; siehe dazu Nr. 2.2.2 in diesem Bericht.

(7) Gegen die Verpflichtung der Standesbeamten, bei Eintragungen über Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten, habe ich Bedenken geltend gemacht (4. TB S. 44). Der Bundesminister des Innern erwägt, die Dienstanweisung für die Standesbeamten unter datenschutzrechtlichen Aspekten zu überprüfen; siehe dazu Nr. 2.2.5 in diesem Bericht.

(8) Gegen die Registrierung der Fernsprechnummer des angerufenen Gesprächsteilnehmers bei dienstlichen und privaten Telefongesprächen, die von Dienstapparaten aus geführt werden, habe ich Bedenken angemeldet und andere Mittel zur Kontrolle vorgeschlagen (4. TB S. 39 f.). Weder der Bundesminister des Innern noch der für die entsprechenden Vorschriften zuständige Bundesminister der Finanzen haben die Bereitschaft erkennen lassen, diesen Bedenken Rechnung zu tragen; siehe dazu Nr. 2.4.5 in diesem Bericht.

(9) Um eine Trennung der Beihilfeakten von den übrigen Personalakten zu erreichen, hatte ich den Bundesminister des Innern um eine Änderung des entsprechenden Erlasses aus dem Jahre 1966 gebeten (4. TB S. 39). Eine abschließende Antwort liegt auch deswegen noch nicht vor, weil meine Kompetenz in dieser Frage bestritten wird.

(10) Bei der Bundesversicherungsanstalt für Angestellte wurden Mängel, insbesondere bei der Datensicherung, festgestellt (4. TB S. 13). Diese Mängel sind im wesentlichen behoben, siehe dazu Nr. 2.13.2 in diesem Bericht.

(11) Auf das Fehlen einer Übersicht gemäß § 15 Nr. 1 BDSG in der Arbeitsverwaltung und auf die Vorarbeiten dazu wurde hingewiesen (4. TB S. 18). Die Übersicht ist inzwischen erstellt.

(12) Mängel bei den technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes bei der Bau-Berufsgenossenschaft (Bau-BG) Hamburg hatte ich beanstandet (4. TB S. 16 f.). Die Bau-BG hat erklärt, daß die Mängel behoben werden; eine Nachfolgeprüfung, die auch die Sicherungsmaßnahmen im

inzwischen bezogenen Neubau einschließen wird, ist für das Frühjahr 1983 geplant.

(13) Gegen die Angabe des Zahlungsgrundes (z. B. „Arbeitslosenhilfe") auf Überweisungsträgern der Bundesanstalt für Arbeit hatte ich Bedenken geltend gemacht (4. TB S. 19). Ich habe mich davon überzeugt, daß diese Angaben weiterhin erforderlich sind, um den Pfändungsschutz für die Leistungen sicherzustellen.

(14) Auf die Gefahren einer Zentraldatei mehrerer Sozialleistungsträger mit Daten über ärztliche Untersuchungen habe ich hingewiesen (4. TB S. 45). Erwartungsgemäß ist die Einrichtung einer solchen Zentraldatei durch Gesetz ausgeschlossen worden; siehe dazu Nr. 2.11.1 in diesem Bericht.

(15) Auf unzulässige, durch Übertragungsfehler ausgelöste Übermittlungen vom Kraftfahrt-Bundesamt an Adressenverlage habe ich hingewiesen (4. TB S. 21). Das Problem hat sich weitgehend entschärft; siehe dazu Nr. 2.7.1 in diesem Bericht.

(16) Auf die Notwendigkeit einer fristgerechten Tilgung von Eintragungen im Verkehrszentralregister habe ich hingewiesen (4. TB S. 21). Eine Lösung, die dies ohne erheblichen Mehraufwand sichert, ist noch nicht gefunden; siehe dazu Nr. 2.7.1 in diesem Bericht.

(17) Eine zu weitgehende Erhebung von Berufs- und Gewerbeangaben bei der Kraftfahrzeugzulassung hatte ich beanstandet (4. TB S. 21). Die vom Bundesminister für Verkehr seinerzeit zugesagte Neuregelung ist noch nicht erfolgt; siehe dazu Nr. 2.7.1 in diesem Bericht.

(18) Für den direkten Zugriff der Polizeibehörden auf Datenbestände des Kraftfahrt-Bundesamtes habe ich eine gesetzliche Regelung gefordert (4. TB S. 20 f.). Wegen des fortgeschrittenen Ausbaustadiums des Zentralen Verkehrsinformationssystems (ZEVIS) ist die Entscheidung des Gesetzgebers noch dringlicher geworden; siehe dazu Nr. 2.7.2 in diesem Bericht.

(19) Für den Erlaß eines Archivgesetzes hatte ich Grundsätze formuliert (4. TB S. 50 f.). Der inzwischen erstellte Referentenentwurf für ein Bundesarchivgesetz entspricht diesen Grundsätzen überwiegend, ist in einigen Punkten jedoch zu kritisieren; siehe dazu Nr. 2.9 in diesem Bericht.

(20) Bei der Prüfung der Deutschen Bundesbank hatten sich einzelne Mängel ergeben (4. TB S. 19 f.). Die notwendigen Maßnahmen wurden im abgelaufenen Jahr ergriffen; nur in einem Punkt sind sie noch nicht abgeschlossen; siehe dazu Nr. 2.17.3 in diesem Bericht.

(21) Zur Praxis der Bankauskünfte hatte ich mich kritisch geäußert (4. TB S. 40). Nachdem auch von Seiten der anderen Datenschutz-Kontrollinstanzen für den öffentlichen wie auch für den nicht-öffentlichen Bereich datenschutzrechtliche Bedenken erhoben worden sind, werden nunmehr gemeinsame Verhandlungen mit den Spitzenverbänden der Kreditwirtschaft angestrebt; siehe dazu Nr. 2.17.4 d in diesem Bericht.

(22) Zum Schutz von Mietinteressenten vor exzessiven Fragebögen habe ich eine gesetzliche Regelung angeregt (4. TB S. 45). Der Bundesminister der Justiz hat dazu eine abwartende Haltung eingenommen; siehe dazu Nr. 4.3.1 in diesem Bericht.

(23) Fünfundzwanzig Fallgruppen von unzulässiger bzw. nicht mehr zulässiger Datenverarbeitung durch das Bundeskriminalamt (BKA) wurden beanstandet (4. TB S. 22). In allen Fällen teilt der Bundesminister des Innern meine Rechtsauffassung und hat die Beanstandungen anerkannt. Die entsprechenden Löschungen und Verfahrensänderungen sind vorgenommen oder eingeleitet; siehe dazu Nr. 3.3.8 in diesem Bericht.

(24) Auf die problematische Speicherung von Daten über „andere Personen", d. h. von weder beschuldigten noch verdächtigten Bürgern in den PIOS-Dateien des BKA wurde hingewiesen (4. TB S. 23). Dieses Problem hat durch die Einrichtung weiterer PIOS-Dateien an Bedeutung zugenommen; siehe dazu Nr. 3.3.8 in diesem Bericht.

(25) Die Speicherung von Daten im Rahmen der Häftlingsüberwachung, die über bestimmte Auswahlkriterien hinausgingen, wurde beanstandet (4. TB S. 25). Eine inzwischen erfolgte neue Regelung kommt den datenschutzrechtlichen Bedenken entgegen; siehe dazu Nr. 3.3.8 in diesem Bericht.

(26) Zur Rasterfahndung und zur polizeilichen Beobachtung hatte ich auf Defizite bei den Rechtsgrundlagen hingewiesen (4. TB S. 52). Diese Defizite bestehen noch immer.

(27) Eine Revision der Richtlinien über die erkennungsdienstliche Behandlung wurde gefordert (4. TB S. 26). Neue Richtlinien, die den datenschutzrechtlichen Belangen entgegenkommen, sind verabschiedet; siehe dazu Nr. 3.3.6 in diesem Bericht.

(28) Auf ungeregelte Datenschutzprobleme bei INTERPOL wurde hingewiesen (4. TB S. 26 f.). Inzwischen hat INTERPOL seine Statuten um einen Datenschutzteil ergänzt, der dazu beitragen kann, daß die Lösung der Probleme vorangetrieben wird. Eine unabhängige Kontrollinstanz ist bisher jedoch nicht vorgesehen; siehe dazu Nr. 3.3.9 in diesem Bericht.

(29) Für die Weitergabe von Informationen durch die Polizei an den Verfassungsschutz habe ich eine analoge Einhaltung des Rahmens von § 7 Abs. 3 G 10 gefordert (4. TB S. 28). Diese Frage ist nach wie vor strittig.

(30) Die Verarbeitung von Informationen durch den Verfassungsschutz, die aus Hausdurchsuchungen und Telefonüberwachungsmaßnahmen der

Polizei stammen, hatte ich beanstandet (4. TB S. 29). Hierzu ist noch keine abschließende Stellungnahme des Bundesministers des Innern eingegangen; siehe dazu Nr. 3.5 in diesem Bericht.

(31) An der Erforderlichkeit einer Sonderdatei des Verfassungsschutzes habe ich Zweifel geäußert (4. TB S. 28). Der Bundesminister des Innern hat eine Überprüfung eingeleitet, deren Ergebnis mir noch nicht vorliegt; siehe dazu Nr. 3.5 in diesem Bericht.

(32) Eine erneute Kontrolle der Praxis der Dateianfrage im Rahmen der Sicherheitsüberprüfung wurde angekündigt (4. TB S. 29). Wegen ungeklärter Fragen des Umfangs meiner Kontrollkompetenz konnte die Kontrolle im Berichtsjahr nicht durchgeführt werden; siehe dazu Nr. 3.5 in diesem Bericht.

(33) Die praktische Auswirkung der Neuregelung der Amtshilfe des Bundesgrenzschutzes (BGS) für die Nachrichtendienste sollte noch geprüft werden (4. TB S. 31). Die begonnene Prüfung mußte wegen Meinungsverschiedenheiten mit dem Bundesamt für Verfassungsschutz über den Umfang meiner Kontrollkompetenz unterbrochen und konnte erst kurz vor Weihnachten zu Ende geführt werden. Die Auswertung ist noch nicht abgeschlossen; siehe dazu Nr. 3.5 in diesem Bericht.

(34) Über Gespräche zur Präzisierung von Weisungen für die Arbeit des Militärischen Abschirmdienstes habe ich berichtet (4. TB S. 32 f.). Die in diesem Jahr fortgesetzten Gespräche haben zu Fortschritten für den Datenschutz geführt.

(35) Gegen den Zugriff von Polizeidienststellen, die keine zollrechtlichen Aufgaben wahrnehmen dürfen, auf die Daten aus der zollrechtlichen Überwachung habe ich erhebliche Bedenken dargelegt (4. TB S. 33). Trotz ausführlicher Diskussion ist eine Änderung dieser Praxis nicht abzusehen; siehe dazu Nr. 3.8.3 in diesem Bericht.

(36) Über die Weigerung des Bundesministers der Finanzen (BMF), mir beim Zollkriminalinstitut (ZKI) eine Prüfung zu ermöglichen, ob und unter welchen Umständen ca. 900 Datensätze aus der polizeilichen Beobachtung im Polizeibestand aus rechtlichen Gründen gelöscht und im gleichartig verfügbaren Bestand des ZKI neu eingespeichert wurden, habe ich berichtet (4. TB S. 34). Der BMF bestreitet nach wie vor, daß mir der Zugang zu diesen Angaben zusteht.

Sachregister

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
AGK	Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung
Amtsbl.	Amtsblatt
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS-Innere-Sicherheit
APLF	Arbeitsdatei PIOS-Landfriedensbruch und verwandte Straftaten
APLV	Arbeitsdatei PIOS-Landesverrat
APSF	Arbeitsdatei PIOS-Staatsgefährdung
APW	Arbeitsdatei PIOS-Waffen
AZR	Ausländerzentralregister
BASt	Bundesanstalt für Straßenwesen
BAT	Bundes-Angestelltentarifvertrag (Bund, Länder, Gemeinden)
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BdO	Bundesverband der Ortskrankenkassen
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BFS	Bundesanstalt für Flugsicherung
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKAAN	Aktennachweis des BKA
BKAG	Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes
BKA-St	Abteilung Staatsschutz beim Bundeskriminalamt
BMA	Bundesminister für Arbeit und Sozialordnung
BMF	Bundesminister der Finanzen
BMI	Bundesminister des Innern
BMP	Bundesminister für das Post- und Fernmeldewesen
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BMWi	Bundesminister für Wirtschaft
BND	Bundesnachrichtendienst
BPersVG	Bundespersonalvertretungsgesetz
BRRG	Rahmengesetz zur Vereinheitlichung des Beamtenrechts — Beamtenrechtsrahmengesetz
BStatG	Bundesstatistikgesetz
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgesetz
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BWO	Bundeswahlordnung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
CoArb	Computergestützte Arbeitsvermittlung
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden
DAV	Allgemeine Verwaltungsvorschrift für die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Amtsverwaltung (Dienstanschlußvorschriften)
DFVLR	Deutsche Forschungs- und Versuchsanstalt für Luft- und Raumfahrt e. V.
DISPOL	Digitales Sondernetz der Polizei
DSL-Bank	Deutsche Siedlungs- und Landesrentenbank
DV	Datenverarbeitung
DVA	Datenverarbeitungsanlage
DVDIS	„Datenerfassung, Verarbeitung, Dokumentation und Informationsverbund" in den sozialärztlichen Diensten mit Hilfe der EDV
ed-Unterlagen	erkennungsdienstliche Unterlagen
EDV	Elektronische Datenverarbeitung
EWS	Elektronisches Wählsystem
FDR	Falldatei Rauschgift
FGER	Falldatei Geiselnahme, Erpressung, Raub
FVD	Fachvermittlungsdienst

G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GG	Grundgesetz
GSD	Grenzschutzdirektion
IDVS II	Informations- und Datenverarbeitungssystem für die Ortskrankenkassen
IMK	Innenministerkonferenz
INPOL	Informationssystem der Polizei
INZOLL	Informationssystem für den Zollfahndungsdienst
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KfW	Kreditanstalt für Wiederaufbau
KpS-Richtl.	Richtlinien über die Errichtung und Führung kriminalpolizeilicher personenbezogener Sammlungen
KVKG	Krankenversicherungs-Kostendämpfungsgesetz
LAB	Lastenausgleichsbank
LED	Leistungsempfängerdatei
MAD	Militärischer Abschirmdienst
MDR	Monatsschrift für Deutsches Recht
MiStra	Anordnung über Mitteilungen in Strafsachen
MiZi	Anordnung über Mitteilungen in Zivilsachen
MRRG	Melderechtsrahmengesetz
MTB	Manteltarifvertrag für Arbeiter des Bundes
NADIS	Nachrichtendienstliches Informationssystem
OCR-Belege	Belege mit genormter, optisch und automatisch lesbarer Schrift (optical character recognition)
PERFIS	Personalführungs- und Informationssystem Soldaten
PDV	Polizeidienstvorschrift
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PZD	Personenzentraldatei
REHA	Rehabilitation
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RVO	Reichsversicherungsordnung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB	Sozialgesetzbuch
SGB X	Zehntes Buch Sozialgesetzbuch
SPUDOK	Spurendokumentationssystem
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht
TESCH	Datei zur Auswertung extremistischen und terroristischen Schriftguts
TÜV	Technischer Überwachungsverein
USG	Unterhaltssicherungsgesetz
VDR	Verband Deutscher Rentenversicherungsträger
VG	Verwaltungsgericht
VkBl	Verkehrsblatt
VNP	Vorgangsnachweis Personen
VwGO	Verwaltungsgerichtsordnung
VZR	Verkehrszentralregister
WRV	Weimarer Reichsverfassung
WSD	Wasser- und Schiffahrtsdirektion
ZBR	Zeitschrift für Beamtenrecht
ZEVIS	Zentrales Verkehrsinformationssystem
ZKI	Zollkriminalinstitut
ZPI	Zentraler Personenindex
ZPO	Zivilprozeßordnung
ZÜ	Zollrechtliche Überwachung

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 08 21, Herderstraße 56, 5300 Bonn 2, Telefon (02 28) 36 35 51
ISSN 0722-8333